Kaseya 2

# Configuração de monitoramento

## Guia do usuário

Version R8

Português

Outubro 23, 2014

## Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

# Conteúdo

# Introdução

O módulo **Monitoramento** no **Virtual System Administrator™** fornece seis métodos para monitorar máquinas e arquivos de logs:

- **Alertas**: monitora eventos nas máquinas do *agente*.
- **Alertas de log de eventos**: monitora eventos nos logs de eventos das máquinas do *agente*.
- **Conjuntos de monitores**: monitora o estado de desempenho nas máquinas do *agente*.
- **Conjuntos SNMP**: monitora o estado de desempenho nos *dispositivos sem agente*.
- **Verificação do sistema**: monitora eventos em máquinas *sem agente*.
- **Monitoramento de Registros** - Monitora eventos nos *arquivos de registro*.

Este guia de início rápido fornece uma introdução aos cinco primeiros métodos gerais de monitoramento e notificação. Consulte o guia de início rápido **Como configurar analisadores de logs passo a passo** *(http://help.kaseya.com/webhelp/PTB/VSA/R8/PTB_logparsers_R8.pdf#zoom=70&navpanes=0)* para obter informações sobre o monitoramento de arquivos de log.

> **Nota:** Você pode aplicar configurações de monitor rapidamente a uma organização *por política* usando o **assistente de configuração** *(http://help.kaseya.com/webhelp/PTB/SSP/R8/index.asp#11220.htm)* do **Standard Solution Package**.
>
> **Nota:** Consulte o **guia de início rápido** *(http://help.kaseya.com/webhelp/PTB/KNM/R8/PTB_knmquickstart_R8.pdf#zoom=70&navpanes=0)* do **Network Monitor** para obter uma introdução ao monitoramento de máquinas e dispositivos *sem agentes*.

# Termos e conceitos de monitores

Os mesmos termos e conceitos do gerenciamento de alertas se aplicam a todos os métodos de monitoramento.

## Alertas e alarmes

- **Alertas** - Um alerta é criado quando o desempenho de uma máquina ou dispositivo corresponda a critérios ou "condições de alerta" predefinidos.
- **Alarmes**: *alarmes* são uma maneira gráfica de notificar o usuário sobre a ocorrência de um *alerta*. Em muitas exibições gráficas do VSA, quando um alerta existe, o VSA exibe, por padrão, um ícone de luz vermelha de tráfego. Se não há alertas, um ícone de luz verde de tráfego é exibido. Esses ícones podem ser personalizados.
- **Logss**: dois logs se distinguem entre alertas e alarmes.
  - **Log de alarmes**: acompanha qualquer *alarme que foi criado por um alerta.*
  - **Log de ações dos monitores**: acompanha qualquer *alerta que foi criado*, se um alarme ou qualquer outra ação tiver sido tomada ou não em resposta para aquele alerta.

## Ações

**Criar um alarme** representa somente um *tipo de ação* que pode ser tomada quando um alerta ocorrer. Dois outros tipos de ações são notificações, que podem ser **enviar um e-mail** ou **criar um ticket**. Um quarto tipo de ação é **executar um procedimento do agente** para responder automaticamente ao alerta. Estes quatro tipos de ações são denominados **Código ATSE**. Se atribuído a uma ID de máquina, ID de grupo ou a um dispositivo SNMP, o código ATSE indica quais tipos de ações serão tomadas para o alerta definido.

- A = Criar **a**larme
- T = Criar **t**icket
- S = Executar procedimento do agente
- E = Destinatários de **e**-mail

Nenhuma das ações ATSE são necessárias. Tanto a ação de alerta quanto a ação ATSE, não incluindo ações, são reportadas no Centro de informações > Monitor - Relatório do Log de ações do monitor.

## Tipos de alertas

Os tipos de alertas incluem:

- Discovery > **LAN Watch** *(http://help.kaseya.com/webhelp/PTB/KDIS/R8/index.asp#1944.htm)*
- Backup > Alertas de backup
- Monitor > Alertas: estes são alertas "fixos" especializados que estão prontos para serem aplicados a uma máquina.
- Monitor > Atribuir monitoramento
- Monitor > Alerta de interceptações SNMP
- Monitor > Atribuir SNMP
- Monitor > Verificações do sistema
- Monitor > Resumo do analisador
- Monitor > Atribuir conjuntos de analisadores
- Gerenciamento de correções > Alertas de correções
- Controle remoto > Alertas fora do local
- Segurança > Aplicar conjuntos de alarmes

Outros módulos complementares têm alertas que não estão enumerados aqui.

## Seis métodos de monitoramento

Cada um dois seis métodos de monitoramento no **Virtual System Administrator™** baseia-se *no evento* ou *no estado*.

- Baseado em eventos
  - **Alertas**: monitora eventos nas máquinas do *agente*
  - **Alertas de log de eventos**: monitora eventos nos logs de eventos das máquinas *instaladas no agente*
  - **Verificação do sistema**: monitora eventos em máquinas *sem agente*
  - **Monitoramento de Registros** - Monitora eventos nos *arquivos de registro*.
- Baseado em estado
  - **Conjuntos de monitores**: monitora o estado de desempenho nas máquinas do *agente*
  - **Conjuntos SNMP**: monitora o estado de desempenho nos *dispositivos sem agente*

## Alertas baseados em eventos

Alertas, Verificação do sistema, **Alertas do log de eventos** *(página 7)* e Monitoramento de logs representam **alertas baseados em eventos** que ocorrem possivelmente uma única vez. Por exemplo, um backup pode falhar. Mesmo que o backup seja posteriormente bem-sucedido, a falha do backup é um evento histórico no log do alarme. Se um alarme é criado para este tipo de evento, o *alarme permanece "aberto" no log do alarme mesmo que a condição do alerta se recupere.* Normalmente, você utiliza a página Resumo de alarmes para revisar alarmes criados por alertas baseados em eventos. Quando o problema é resolvido, você "fecha" o alarme.

Alertas baseados em eventos são normalmente mais fáceis de configurar, já que as possibilidades são reduzidas a um ou mais eventos que aconteceram ou não dentro de um período específico.

## Alertas baseados no estado

Processos, serviços e contadores do conjunto de monitores e objetos do conjunto SNMP estão atualmente dentro ou fora do intervalo do estado esperado deles e são exibidos como ícones de alarme verde ou vermelho de forma *dinâmica* nos dashlets de monitoramento. Estes são conhecidos como **alertas baseados no estado**.

- *Se uma condição de alerta existe atualmente, os dashlets do monitor exibem um ícone de alarme vermelho.*
- *Se uma condição de alerta não existe atualmente, os dashlets do monitor exibem um ícone de alarme verde.*

Se você criar um alarme para alertas baseados no estado, eles criarão entradas de alarme no log de alarmes do mesmo modo que alarmes baseados em eventos, que você, então, pode escolher fechar. Porém, como alertas baseados no estado normalmente entram e saem de uma condição de alerta dinamicamente, você deve evitar criar um alarme sempre que isso acontecer. Em vez disso, utilize o dashlet Status de rede para identificar o *status atual* de alertas baseados no estado. Após o problema ter sido corrigido na máquina ou dispositivo, o status do alerta retorna automaticamente a um ícone verde. Você não precisa "fechar" manualmente o alerta neste dashlet.

> **Nota:** Se você decidir criar alarmes tradicionais para conjuntos de monitores e alertas off-line de modo específico, estes dois tipos de alertas poderão ser fechados automaticamente quando se recuperarem. Veja a caixa de seleção **Permitir encerramento automático de alarmes e tickets** na página Sistema> Configurar.

Os alarmes baseados em estado geralmente requerem mais trabalho na configuração que os alarmes baseados em eventos porque o objetivo é medir o nível do desempenho em vez de indicar a falha.

## Painéis e dashlets

A página **Lista de painéis** é o principal método do VSA de exibir visualmente dados de monitoramento, incluindo alertas e alarmes. A página **Lista de Painéis** mantém janelas de monitoramento configuráveis denominadas **Visualizações de Painel**. Cada painel contém um ou mais painéis de dados de

monitoramento denominados **Painéis**. Cada usuário do VSA pode criar seus próprios painéis personalizados. Os tipos de dashlets incluem:

- Lista de Alarmes
- Status da Rede de Alarmes
- Rotor de alarmes
- Registrador de alarmes
- Status da rede
- Status do grupo de alarmes
- Status do conjunto de monitores
- Status do Monitor
- Máquinas on-line
- N Principais - Gráfico de Alarmes do Monitor

## Como revisar alarmes

Todas as condições de alertas que tenham a caixa de seleção **Criar alarme** marcada — tanto alarmes baseados em eventos quanto alarmes baseados em estado — são registrados no **log de alarmes**. Um alarme listado no log de alarmes não representa o *status atual* de uma máquina ou dispositivo, pelo contrário, ele é um *registro* de um alarme que ocorreu *no passado*. Um log de alarmes permanece `Open` até que você o fecha.

Os alarmes criados podem ser revistos, `Closed` ou **excluídos...** em:

- Monitor > Resumo de alarmes
- Monitor > Lista de painéis > qualquer Janela de resumo de alarmes dentro de um dashlet
- Agente > Logs de agentes > Log de alarmes
- Live Connect > Dados de agentes > Logs de agentes > Log de alarmes

Os alarmes criados também podem ser examinados usando:

- Monitor > Lista de painéis > Lista de alarmes
- Monitor > Lista de painéis > Status da rede de alarmes
- Monitor > Lista de painéis > Rotor de alarmes
- Monitor > Lista de painéis > Registrador de alarmes
- Monitor > Lista de painéis > Status de alarmes do grupo
- Monitor > Lista de painéis > Status dos conjuntos de monitores
- Monitor > Lista de painéis > Status de monitores
- Monitor > Lista de painéis > Principais N - Contagem de alarmes de monitores
- Monitor > Lista de painéis > KES Status
- Monitor > Lista de painéis > KES Ameaças
- Centro de informações > Emissão de relatórios > Relatórios > Monitoramento > Logs > Log de alarmes
- Centro de informações > Emissão de relatórios > Relatórios > Monitoramento > Log de ações do monitor

## Como verificar o desempenho (com ou sem a criação de alarmes)

Você pode verificar o *status atual* dos resultados de desempenho dos conjuntos de monitores e conjuntos SNMP, *com ou sem a criação de alarmes*, em:

- Monitor > Contador ao vivo
- Monitor > Log de monitores
- Monitor > Log SNMP
- Monitor > Painel > Status de rede
- Monitor > Painel > Status de alarmes do grupo
- Monitor > Painel > Status do conjunto de monitoramento

- Centro de informações > Emissão de relatórios > Relatórios > Monitoramento > Logs

## Suspender Alarmes

O acionamento de alarmes pode ser suspenso. A página **Suspender Alarmes** suprime alarmes por períodos especificados, como períodos recorrentes. Isso permite que a atividade de atualização e manutenção ocorra sem gerar alarmes. Quando os alarmes estão suspensos para uma ID de máquina, *o agente ainda coleta dados, mas não gera alarmes correspondentes.*

## Alarmes do grupo

Os alarmes para alertas, alertas do log de eventos, verificação do sistema e monitoramento de logs são automaticamente atribuídos à categoria **alarme do grupo**. Se um alarme é criado, o alarme do grupo ao qual ele pertence é acionado também. As categorias de alarmes de grupos dos conjuntos de monitores e conjuntos SNMP são atribuídas manualmente quando os conjuntos são definidos. Os alarmes dos grupos são exibidos no dashlet Status do alarme do grupo da página Monitor > **Lista de painéis**. Você pode criar novos grupos utilizando a guia **Nomes da colunas dos alarmes dos grupos** em Monitor > Listas de monitores. Nomes das colunas de alarmes de grupo são atribuídos aos conjuntos de monitores usando Definir Conjunto de Monitores.

# Alertas

A página **Alertas** permite que você defina alertas rapidamente para as condições de alertas tipicamente encontradas no ambiente de TI.  Por exemplo, pouco espaço em disco é geralmente um problema nas máquinas gerenciadas. Selecionar o tipo de alerta do `Low Disk` exibe um campo adicional que deixa que você define o limite de `% free space`. Após definido, você pode aplicar este alerta imediatamente para qualquer ID de máquina exibida na página **Alertas** e especificar ações a tomar em resposta ao alerta.

Há múltiplos tipos de alertas disponíveis.

## Tipos de alertas

- A página **Alertas - Resumo** mostra quais alertas estão ativados em cada máquina. É possível aplicar ou limpar configurações ou copiar configurações de alertas ativados.
- A página **Alertas - Status do agente** alerta quando um agente está off-line, fica on-line pela primeira vez ou se alguém desabilitou o controle remoto na máquina selecionada.
- A página **Alerta sobre alterações em aplicativos** alerta quando um novo aplicativo é instalado ou removido nas máquinas selecionadas.
- A página **Alertas - Obter Arquivo** alerta quando um comando **getFile()** ou **getFileInDirectoryPath()** executa, carrega o arquivo, e o arquivo passa a ser diferente da cópia previamente armazenada no servidor da Kaseya. Se não havia cópia anterior no servidor da Kaseya, o alerta é criado.
- A página **Alertas - Alterações de hardware** alerta quando uma configuração de hardware se altera nas máquinas selecionadas. As alterações de hardware detectadas incluem a adição ou remoção de RAM, dispositivos PCI e unidades de disco rígido.
- A página **Alertas - Pouco espaço em disco** alerta quando o espaço em disco disponível cai abaixo de um porcentual específico de espaço livre em disco.
- A página **Alertas de log de eventos** alerta quando uma entrada no log de eventos para uma máquina selecionada corresponde a critérios específicos. Após selecionar o **tipo de log de eventos**, você pode filtrar as condições de alerta especificadas por **conjunto de eventos** e por **categoria de eventos**.
- A página **Alertas - Falha no procedimento do agente** alerta quando a execução de um procedimento falha em uma máquina gerenciada.
- A página **Alertas - Violação da proteção** alerta quando um arquivo é alterado ou caso se detecte uma violação de acesso em uma máquina selecionada.
- A página **Alertas - Novo agente instalado** alerta quando um novo agente é instalado em uma máquina gerenciada por *grupos de máquinas* selecionados.
- A página **Alertas - Alerta de correções** alerta para eventos de gerenciamento de correções em máquinas gerenciadas.
- A página **Alertas - Alerta de backup** alerta por eventos de backup em máquinas gerenciadas.
- A página **Alertas - Sistema** alerta para eventos selecionados que ocorrem no *servidor da Kaseya*.

## Para criar um alerta

O mesmo procedimento geral se aplica a todos os tipos de alertas.

1. Selecione uma função de alerta na lista suspensa **Selecionar Função de Alerta**.
2. Marque estas caixas de seleção para realizar suas ações correspondentes quando uma condição de alerta for encontrada:
   - Criar um **a**larme
   - Criar **t**icket
   - Executar o **s**cript
   - Destinatários de **e**-mail
3. Definir parâmetros adicionais para e-mails.

4. Definir parâmetros adicionais específicos para alertas. Podem diferir de acordo com a função de alerta selecionada.
5. Marque as linhas de paginação às quais aplicar o alerta.
6. Clique no botão **Aplicar**.

### Para cancelar um alerta

1. Selecione uma ou mais linhas de paginação.
2. Clique no botão **Limpar**.

   As informações do alerta listadas ao lado da linha de paginação serão removidas.

# Alertas de Log de Eventos

A página **Alertas de logs de eventos** é um dos tipos mais avançados de alertas e requer configuração especial. Ele começa com uma boa compreensão de **registros de eventos**.

# Registros de eventos

Um **serviço de registro de eventos** é executado nos sistemas operacionais Windows (não disponível com Win9x). O serviço do registro de eventos permite que mensagens sobre eventos de registro sejam emitidas pelo Window de acordo com os programas e componentes. Esses eventos são armazenados nos registros de eventos localizados em cada máquina. Os logs de eventos das máquinas gerenciadas podem ser armazenados no banco de dados do servidor da Kaseya, servir de base para os alertas e relatórios e ser arquivados.

Dependendo do sistema operacional, os **tipos de registro de eventos** disponíveis incluem, mas não estão limitados a:

- Registro de aplicativos
- Registro da segurança
- Registro do sistema
- Registro do Serviço de diretórios
- Registro do Serviço de replicação de arquivos
- Registro do Servidor DNS

Os eventos do Windows são classificados por estas **categorias de registro de eventos**:

- Erro
- Aviso
- Informações
- Auditoria de sucesso
- Auditoria de falha
- Crítico: se aplica somente ao Vista, Windows 7 e Windows Server 2008
- Detalhado: se aplica somente ao Vista, Windows 7 e Windows Server 2008

Os logs de eventos são usados ou referenciados por estas páginas do VSA:

- Monitor > Logs do agente
- Monitor > Alertas do log de eventos
- Monitor > Alertas do log de eventos > Editar conjuntos de eventos
- Monitor > Atualizar listas por varredura
- Agente > Histórico de logs
- Agente > Configurações do log de eventos
- Agente > Logs do agente

- Relatórios > Logs
- Visualizador de eventos do Live Connect >
- Visualização rápida > Visualizador de eventos
- Sistema > Visualizações do banco de dados > vNtEventLog

# Criação de conjuntos de eventos a partir das entradas no log de eventos

Um ícone  de assistente do monitor é exibido próximo às entradas de log do evento no VSA e no **Live Connect**. Passar o curso sobre o ícone de assistente do monitor de uma entrada de log exibe um assistente. Esse assistente permite que você crie um novo critério de conjunto de eventos baseado naquela entrada de log. O novo critério de conjunto de eventos pode ser adicionado a qualquer conjunto de eventos, novo ou existente. O conjunto de eventos novo ou alterado é imediatamente aplicado à máquina que serve como a origem de uma entrada de log. Alterar um conjunto de eventos existente afeta todas as máquinas atribuídas para usar aquele conjunto de eventos. O ícone do assistente do monitor é exibido em:

- Agente > Logs do agente
- Live Connect > Visualizador de eventos
- Live Connect > Dados do agente > Log de eventos

Consulte Monitor > Alertas de log de eventos para obter uma descrição de cada campo exibido no assistente.

# Conjuntos de eventos de amostra

Uma lista crescente de conjuntos de eventos de amostra é fornecida. Os nomes dos conjuntos de eventos de amostra começam com ZC. É possível modificar conjuntos de eventos de amostra, mas a melhor prática é copiar um conjunto de eventos de amostra e personalizar a cópia. Os conjuntos de eventos de amostra estão sujeitos a ser substituídos sempre que os conjuntos de amostras forem atualizados durante um ciclo de manutenção.

# Atribuindo conjuntos de eventos

Você aplica conjuntos de eventos a IDs de máquinas de destino usando a página Monitor > Alertas de logs de eventos.

### Criação de um alerta de registro de eventos

1. Na página Monitor > **Alertas do log de eventos** selecione a guia **Atribuir conjunto de eventos**.
2. Selecione um item da lista suspensa **Selecionar tipo de log de eventos**.
3. Selecione o filtro Conjunto de Eventos usado para filtrar os evento que acionarão os alertas. Por padrão, `<All Events>` é selecionado.

   > **Nota:** Você pode criar um novo conjunto de eventos ou editar um conjunto de eventos existente ao clicar no botão **Editar**.

4. Marque a caixa ao lado de qualquer destas **categorias de eventos**:
   - Erro
   - Aviso

- Informações
- Auditoria de sucesso
- Auditoria de falha
- Crítico: se aplica somente ao Vista, Windows 7 e Windows Server 2008
- Detalhado: se aplica somente ao Vista, Windows 7 e Windows Server 2008

> **Nota:** Letras vermelhas indicam conexão desabilitada. A coleta de logs de eventos pode ser desabilitada pelo VSA para uma máquina específica, com base nas configurações definidas em Agente > Configurações do log de eventos. Uma categoria de evento específica (EWISFCV) pode não estar disponível para certas máquinas, assim como as categorias de eventos Crítico e Detalhado. **Alertas de log de eventos ainda são gerados mesmo que os logs de eventos não sejam coletados pelo VSA.**

5. Especifique a *frequência* da condição do alerta exigida para acionar um alerta:
   - **Alertar quando esse evento ocorrer uma vez.**
   - **Alertar quando este evento ocorrer <N> vezes dentro de <N> <períodos>**.
   - **Alertar quando este evento não ocorrer dentro de <N> <períodos>**.
   - **Ignorar alarmes adicionais para <N> <períodos>**.
6. Clique nas opções **Adicionar** ou **Substituir**.
   - **Adicionar** adiciona o conjunto de eventos selecionado à lista dos conjuntos de eventos já atribuídos para as máquinas selecionadas.
   - **Substituir** substitui a lista inteira de conjuntos de eventos atribuídos em máquinas selecionadas pelo conjunto de eventos selecionado.
7. Selecione a guia **Ações de alerta do conjunto** para selecionar as ações a serem tomadas em resposta à condição de alerta especificada.
8. Clique em **Aplicar** para atribuir alertas de tipo de evento selecionados às IDs de máquinas selecionadas.

> **Nota:** Clique em **Remover** para remover todos os alertas de conjuntos de eventos das IDs de máquinas selecionadas imediatamente. Você não precisa clicar no botão **Aplicar**.

# Editando conjuntos de eventos

Na etapa 2 do procedimento **Criando um alerta do registro de eventos** acima, você precisa selecionar um conjunto de eventos. A discussão a seguir descreve como editar conjuntos de eventos.

**Editar Conjuntos de Eventos** filtra o acionamento de alertas de acordo com o monitoramento de eventos em registros de eventos mantidos pelo sistema operacional Windows de uma máquina gerenciada. É possível atribuir vários conjuntos de eventos a uma ID de máquina.

Os conjuntos de eventos contêm uma ou mais **condições**. Cada condição contém filtros para diferentes campos de uma **entrada do registro de eventos**. Os campos são **origem**, **categoria**, **ID de evento**, **usuário** e **descrição**. Uma entrada no **registro de eventos** *(página 7)* tem de corresponder a todos os filtros de campo de uma condição para ser considerada uma correspondência. Um campo com um asterisco (*) significa que qualquer sequência, como um zero, será considerada uma correspondência. Uma correspondência de qualquer *uma* das condições em um conjunto de eventos é suficiente para acionar um alerta para qualquer máquina a qual o conjunto de eventos esteja aplicado.

> **Nota:** Normalmente, se duas condições são adicionadas a um conjunto de eventos, eles são geralmente interpretados como uma instrução OR. Se uma dessas condições corresponder, o alerta será acionado. A exceção é quando a opção **Alertar quando este evento não ocorrer dentro de <N> <períodos>** é selecionada. Nesse caso, as duas condições devem ser interpretadas como uma instrução E. Ambos *não* devem acontecer dentro do período especificado para acionar um alerta.
>
> **Nota:** Você pode exibir logs de eventos diretamente. Em uma máquina com Windows, clique em **Iniciar**, **Painel de Controle**, **Ferramentas Administrativas** e em **Visualizador de Eventos**. Clique em **Aplicativos**, **Segurança** ou **Sistema** para exibir os eventos nesse registro. Clique duas vezes em um evento para exibir a janela **Propriedades**. Você pode copiar e colar texto da janela **Propriedades** de qualquer evento nos campos **Editar Conjunto de Eventos**.

## Para criar um conjunto de eventos

1. Selecione a página Monitor > **Alertas de logs de eventos**.
2. Selecione um **Tipo de Registro de Eventos** na segunda lista suspensa.
3. Selecione `<New Event Set>` na lista suspensa **Definir eventos para corresponder ou ignorar**. A janela pop-up **Editar Conjunto de Eventos** será exibida. É possível criar um conjunto de eventos:
   - Inserindo um novo nome e clicando no botão **Novo**.
   - Colando os dados do conjunto de eventos como texto.
   - Importando os dados do conjunto de eventos de um arquivo.
4. Se você digitar um novo nome e clicar em **Novo**, a janela **Editar Conjunto de Eventos** exibirá as cinco propriedades usadas para filtrar eventos.
5. Clique em **Adicionar** para adicionar um novo evento ao conjunto de eventos.
6. Clique em **Ignorar** para especificar um evento que *não* deve acionar um alarme.
7. Você pode opcionalmente **Renomear**, **Excluir** ou **Exportar o conjunto de eventos**.

## Condições ignoradas

Se uma entrada do registro de eventos corresponder a uma ou mais **condições a ignorar** em um conjunto de eventos, nenhum alerta será acionado *por um conjunto de eventos*, mesmo se várias condições vários conjuntos de eventos corresponderem a uma entrada do registro de eventos. Como as condições ignoradas substituem *todos os conjuntos de eventos*, é uma boa idéia definir apenas um conjunto de eventos para todas as condições ignoradas, assim você só tem de procurar em um lugar se suspeitar que uma condição ignorada está afetando o comportamento de todos os seus alertas. É necessário atribuir o conjunto de eventos que contém uma condição ignorada a uma ID de máquina para que ele substitua todos os outros conjuntos de eventos aplicados a essa mesma ID de máquina.

*As condições de Ignorar somente substituem os eventos que compartilhem o mesmo tipo de registro.* Portanto, se você criar um "ignore set" para ignorar todas as condições, ele deve ser aplicado várias vezes à mesma ID de máquina, *uma para cada tipo de registro*. Por exemplo, um conjunto de Ignorar aplicado somente como tipo de registro do Sistema não substituirá condições de eventos aplicadas como do tipo de registro de Aplicativo e de Segurança.

1. Selecione a página Monitor > **Alertas de logs de eventos**.
2. Marque a caixa de seleção **Erro** e selecione `<All Events>` na lista do conjunto de eventos. Clique no botão **Aplicar** para atribuir essa configuração a todas as IDs de máquina selecionadas. Isso informa o sistema para gerar um alerta para todos os tipos de eventos de erro. Observe o tipo de registro atribuído.
3. Crie e atribua um "conjunto ignorar evento" a essas mesmas IDs de máquina que especifique todos os eventos que deseja ignorar. O tipo do registro deve corresponder ao tipo do registro na etapa 2.

## Usando o curinga asterisco (*)

Inclua o curinga asterisco (*) com o texto inserido para corresponder a vários registros.Por exemplo:

```
*yourFilterWord1*yourFilterWord2*
```

Isso fará corresponder e criar um alarme para um evento com esta sequência:

```
"This is a test. yourFilterWord1 as well as yourFilterWord2 are in the description."
```

### Exportar e importar Editar eventos

É possível exportar e importar registros do conjunto de eventos como arquivos XML.

- É possível *exportar* um registro de conjunto de eventos existente para um arquivo XML usando a janela pop-up **Editar Conjunto de Eventos**.
- Você pode *importar* um arquivo XML do conjunto de eventos ao selecionar o valor `<Import Event Set>` ou `<New Event Set>` na lista suspensa do conjunto de eventos.

Exemplo:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<event_sets>
 <set_elements setName="Test Monitor Set" eventSetId="82096018">
   <element_data ignore="0" source="*SourceValue*"
      category="*CategoryValue*" eventId="12345"
      username="*UserValue*" description="*DescriptionValue*"/>
 </set_elements>
</event_sets>
```

# Verificações do sistema

O VSA pode monitorar máquinas que *não tenham um agente instalado*. Essa função é executada inteiramente em uma única página denominada **Verificação do Sistema**. As máquinas sem agentes são denominadas **sistemas externos.** A uma máquina com agente é atribuída a tarefa de executar a verificação de sistema no sistema externo. A verificação do sistema geralmente determina se um sistema externo está disponível ou não. Os tipos de verificações do sistema incluem: servidor Web, servidor DNS, conexão de portas, ping e personalizada.

# Conjuntos de monitores

Os **conjuntos de monitores** usam **contadores de desempenho** com base no Windows, para fornecer informações sobre quão bem o sistema operacional ou o aplicativo, serviço ou driver está desempenhando. Os dados do contador podem ajudar a determinar gargalos do sistema e efetuar o ajuste fino do desempenho do sistema e do aplicativo. Por exemplo, um servidor pode continuar a funcionar sem gerar quaisquer erros ou avisos nos registros do evento. Mas, os usuários podem se queixar do baixo tempo de resposta do servidor.

> **Nota:** *Os contadores em conjuntos de monitores do VSA se baseiam em dados de estado em tempo real, e não em arquivos de log. Consulte* **Alarmes** *(página 2)* *para obter mais informações.*

### Objetos de desempenho, Instâncias e Contadores

Quando definir os limites do contador nos **conjuntos de monitores** *(página 12)*, é bom lembrar de forma precisa como o Windows e o VSA identificam os componentes que você pode monitorar:

- **Objeto de Desempenho** - Uma coleção lógica de contadores associados a um recurso ou serviço que pode ser monitorado. Por exemplo: processadores, memória, discos físicos e servidores têm seus próprios conjuntos de contadores pré-definidos.
- **Instância de Objeto de Desempenho** - Termo usado para distinguir entre vários objetos de desempenho do mesmo tipo em um computador. Por exemplo: vários processadores ou discos

físicos. O VSA permite que você ignore este campo caso haja somente uma instância de um objeto.

- **Contador de Desempenho** - Um item de dados associado a um objeto de desempenho e, se necessário, à instância. Cada contador selecionado apresenta um valor correspondente a um aspecto determinado que está definido para o objeto e instância do desempenho.

# Conjuntos de monitores

Um conjunto de monitores é um conjunto de **objetos contadores**, **contadores**, **instâncias de contadores**, **serviços** e **processos** usados para monitorar o desempenho das máquinas. Normalmente, o limite é atribuído a cada objeto/instância/contador, serviço ou processo em um conjunto de monitores. Os alarmes podem ser definidos para acionamento se quaisquer limites no monitor forem excedidos. Um conjunto de monitores deve ser usado como conjunto lógico dos itens a serem monitorados. Um agrupamento lógico, por exemplo, pode servir para monitorar todos os contadores e serviços integrais para a execução de um Exchange Server. É possível atribuir um conjunto de monitores a qualquer máquina que tenha sistema operacional Windows 2000 ou mais recente.

O procedimento geral para trabalhar com conjuntos de monitores é este:

1. Opcionalmente, atualize objetos contadores de conjuntos de monitores, instâncias e contadores manualmente e examine-os usando Listas de Monitores.
2. Crie e mantenha conjuntos de monitores em Monitor > Conjuntos de monitores.
3. Atribua conjuntos de monitores às IDs de máquina em Monitor > Atribuir monitoramento.
4. Opcionalmente, personalize conjuntos de monitores padrão como *conjuntos de monitores individualizados*.
5. Opcionalmente, personalize conjuntos de monitores padrão usando *Autoaprendizado*.
6. Examine os resultados do conjunto de monitores usando:
    - Monitor > Log de monitores
    - Monitor > Contador ao vivo
    - Monitor > Painel > Status de rede
    - Monitor > Painel > Status de alarmes do grupo
    - Monitor > Painel > Status do conjunto de monitoramento
    - Centro de informações > Emissão de relatórios > Relatórios > Monitor > Relatório do conjunto de monitores
    - Centro de informações > Emissão de relatórios > Relatórios > Monitor > Log de ações do monitor

# Conjuntos de monitores de amostra

O VSA fornece uma lista em expansão de conjuntos de monitores de amostra. Os nomes dos conjuntos de monitores de amostra começam com ZC. É possível modificar conjuntos de monitores de amostra, mas a melhor prática é copiar um conjunto de monitores de amostra e personalizar a cópia. Os conjuntos de monitores de amostra estão sujeitos a ser substituídos sempre que os conjuntos de amostras forem atualizados durante um ciclo de manutenção.

# Definindo conjuntos de monitores

Cada conjunto de monitores é definido usando quatro guias.

- A guia **Limites do contador** define as condições do alerta para todos os objetos/instâncias/contadores de desempenho associados ao conjunto de monitores. Estes são os mesmos objetos, instâncias e contadores de desempenho exibidos quando você executa `PerfMon.exe` em uma máquina Windows.
- A guia **Verificação dos Serviços** define as condições de alarmes para um serviço se o serviço em uma ID de máquina parar e opcionalmente tenta reiniciar o serviço interrompido. *O serviço deve ser definido como automático para ser reiniciado por um conjunto de monitores.*
- A guia **Status do processo** definirá as condições de alertas se um processo tiver sido iniciado ou interrompido em uma ID de máquina.
- A guia **Ícones do Monitor** seleciona os ícones do monitor que são exibidos na página Registro do Monitor quando vários estados de alarme ocorrem.

## Configurando os limites do contador

Depois de adicionar um novo conjunto de monitores usando Monitor > **Conjuntos de monitores**, você pode adicionar ou editar limites de contadores usando a guia **Limites do contador**.

Clique em **Adicionar** ou no ícone Editar para usar um assistente que o conduzirá nas seis etapas requeridas para adicionar ou editar um contador de desempenho.

1. Selecione um **Objeto**, **Contador** e, se necessário, uma **Instância** usando suas respectivas listas suspensas.
    - Se somente uma instância de um objeto de desempenho existir, o campo **Instância** normalmente pode ser ignorado.
    - As listas suspensas usadas para selecionar objetos de desempenho, contadores e instâncias são baseadas na "lista principal" mantida usando a página Listas de Monitores. Se um objeto/instância/contador não for exibido em sua respectiva lista suspensa, você pode adicioná-lo manualmente usando **Adicionar Objeto**, **Adicionar Contador** e **Adicionar Instância**.
    - Independentemente do intervalo das instâncias do contador especificado por um conjunto de monitores, a página Log de monitores somente exibe instâncias que existem em uma máquina específica. Instâncias de contadores recentemente adicionadas — por exemplo, a adição de um disco removível a uma máquina — serão exibidas inicialmente na página **Log de monitores** assim que forem detectadas, se incluídas no intervalo especificado para monitoramento por um conjunto de monitores.
    - Quando existirem diversas instâncias, você poderá adicionar uma instância denominada `_Total`. A instância `_Total` significa que você quer monitorar o valor *combinado* de todas as outras instâncias de um objeto de desempenho *como um único contador*.
    - Quando existirem diversas instâncias, você poderá adicionar uma instância de contador denominada `*ALL` para a lista de instâncias compatíveis na guia Listas de monitores > **Instância de contadores**. Ao ter adicionado o contador com o qual deseja trabalhar, o valor `*ALL` será exibido na lista suspensa de instâncias associadas àquele contador. A instância `*ALL` significa que você quer monitorar todas as instâncias para o mesmo objeto de desempenho *com contadores individuais*.
2. Opcionalmente, altere o **Nome** e a **Descrição** do objeto contador padrão.
3. Selecione os dados de registro coletados. Se o valor retornado for numérico, é possível minimizar dados de registro indesejáveis configurando um operador de coleta acima ou abaixo do limite da coleta.
    - **Operador de coleta**: para valores de retorno de sequência de caracteres `Changed`, `Equal` ou `NotEqual`. Para valores numéricos de retorno, as opções são `Equal`, `NotEqual`, `Over` ou `Under`.
    - **Limite de Coleta** - Defina um valor fixo com o qual o valor retornado será comparado, usando o **Operador de Coleta** selecionado, para determinar quais dados do registro serão coletados.
    - **Intervalo de amostra**: define a frequência na qual os dados são enviados pelo agente para o servidor da Kaseya.

4. Especifique quando uma condição de alerta é encontrada.
   - **Operador de alarmes**: para valores de retorno de sequência de caracteres `Changed`, `Equal` ou `NotEqual`. Para valores numéricos de retorno, as opções são `Equal`, `NotEqual`, `Over` ou `Under`.
   - **Limite de alarmes**: define um valor fixo com o qual o valor retornado é comparado, utilizando o **Operador de alarmes** selecionado, para determinar quando uma condição de alerta é encontrada.
   - **Duração**: especifique o horário que os valores retornados devem exceder continuamente o limite do alarme para gerar a condição do alerta. Muitas condições de alerta executam o alarme somente se o nível for sustentado ao longo do período.
   - **Ignorar alarmes adicionais para**: suprime as condições de alerta adicionais para esta mesma emissão durante este período. Isto reduz a confusão de muitas condições de alertas para a mesma emissão.
5. **Avisar quando estiver dentro de X% do limite do alarme**: exibir, opcionalmente, uma condição de alerta de aviso quando o valor retornado estiver dentro de uma porcentagem específica do **Limite de alarme**. O ícone de aviso é um ícone de luz amarela de tráfego .
6. Opcionalmente, ative um **alarme de tendência**. Alarmes de tendência utilizam dados históricos para prever quando a próxima condição de alerta ocorrerá.
   - **Tendência ativada?**- Se afirmativo, uma linha de tendência de regressão linear será calculada de acordo com os últimos 2.500 pontos de dados registrados.
   - **Janela Tendência** - O período usado para estender a linha de tendência calculada para o futuro. Se uma linha de tendência prevista excede o limite do alarme dentro do período futuro específico, uma condição de alerta de tendência é gerada. Normalmente, uma janela de tendências deve ser definida para o tempo que você precisa para se preparar para uma condição de alerta, caso ocorra. Exemplo: um usuário pode desejar um aviso de 10 dias antes que um disco rígido alcance a condição do alerta, para acomodar o pedido, o envio e a instalação de um disco rígido maior.
   - **Ignorar alarmes adicionais de tendência para**: suprime as condições de alerta adicionais de tendência para esta mesma emissão durante este período.
   - Alarmes de tendência são exibidos como um ícone laranja .

   As condições de alerta com status de aviso e as condições de alerta com status de tendência não criam entradas de alarme no log de alarmes, mas alteram a imagem do ícone do alarme em várias janelas de exibição. Você pode gerar um relatório de alarme de tendência em Relatórios > Monitor.

## Configurando as verificações do serviço

Monitore os serviços usando um conjunto de monitores, como segue. Clique em **Adicionar** ou no ícone Editar  para manter um registro da **Verificação dos Serviços**.

1. **Serviço** - Selecione o serviço a ser monitorado na lista suspensa.
   - A lista suspensa se baseia na "lista principal" mantida usando a página Listas de Monitores. Se um serviço não for exibido na lista suspensa, você pode adicioná-lo manualmente usando **Adicionar Serviço**.
   - Você pode adicionar um serviço com o caractere curinga asterisco (`*`) à coluna **Nome** ou **Descrição** na lista de serviços com suporte na guia Listas de monitores > **Serviço**. Quando adicionado, o serviço curinga é exibido na lista suspensa de serviços. Por exemplo, especificar o serviço `*SQL SERVER*` monitorará todos os serviços que incluem a sequência `SQL SERVER` no nome do serviço.
   - Você pode adicionar um serviço denominado `*ALL` à coluna **Nome** ou **Descrição** na lista de serviços com suporte na guia Listas de monitores > **Serviço**. Quando adicionado, o valor `*ALL` é exibido na lista suspensa de serviços. Selecionar o serviço `*ALL` significa que você deseja monitorar todos os serviços.

> **Nota:** Especificar um intervalo de serviços com o caractere curinga * necessita que Permitir correspondência seja marcado.

2. **Descrição** - Descreve o serviço e o motivo do monitoramento.
3. **Tentativas de Reinicialização** - O número de vezes que o sistema deve tentar reiniciar o serviço.
4. **Intervalo de Reinicialização** - O período de tempo de espera entre tentativas de reinicialização. Alguns serviços precisam de mais tempo.
5. **Ignorar alarmes adicionais para**: suprime as condições de alerta adicionais para o período especificado.

### Configurando o status do processo

Clique em **Adicionar** ou no ícone Editar para manter um registro do **Status do Processo**.

1. **Processo** - Selecione o processo a ser monitorado na lista suspensa. A lista suspensa se baseia na "lista principal" mantida usando a página Listas de Monitores. Se um processo não for exibido na lista suspensa, você pode adicioná-lo manualmente usando **Adicionar Processo**.
2. **Descrição** - Descreve o processo e o motivo do monitoramento.
3. **Alarme em transição**: aciona uma condição de alerta quando um processo (aplicativo) é iniciado ou interrompido.
4. **Ignorar alarmes adicionais para**: suprime as condições de alerta adicionais para o período especificado.

# Configurando manualmente os limites do contador - Um exemplo

Neste exemplo, o conjunto de monitores `ZC-PS1-Print Server Monitor` é analisado para ilustrar como os limites do contador dos conjuntos de monitores são definidos.

1. Clique em Monitor > **Conjuntos de monitores** para exibir a primeira página de todos os conjuntos de monitores disponíveis no VSA. Neste caso, foram carregadas amostras de conjuntos de monitores no VSA. Os nomes de amostras do conjunto de monitores começam com um prefixo ZC. Você carrega amostras de conjuntos no VSA em Sistema > **Configurar**.
2. Clique no botão **Editar** ao lado do conjunto de monitores `ZC-PS1-Print Server Monitor`.



**Select the Monitor Set to edit or delete**

<< ZC-EX2- Exchange 2007 Basic >> Add Import Page 3 of 6

| | Name | Description | Group Alarm Column |
|---|---|---|---|
| Edit | ZC-EX2- Exchange 2007 Basic Services - 2 | Basic services for Microsoft Exchange 2007. | |
| Edit | ZC-EX2- Exchange 2007 Service - MSExchangeMonitoring | Service for Microsoft Exchange 2007. | |
| Edit | ZC-EX2- Exchange 2007 Service - MSExchangePop3 | MSExchangePop3 Service for Microsoft Exchange 2007. | |
| Edit | ZC-EX2- Exchange 2007 Service - MSExchangeRepl | MSExchangeRepl service for Microsoft Exchange 2007. | |
| Edit | ZC-FX1-Fax Server Basic Services | Monitor for Faxes sent,Total faxes,Failed faxes,Received faxes & Total ... | |
| Edit | ZC-GMS1-Good Messaging Services | GoodLink Mobile Messaging (Runs GoodLink Mobile Messaging to sync mail to P... | |
| Edit | ZC-IIS2 -IIS Basic Services | Internet Information Service (IIS) Monitoring | |
| Edit | ZC-IIS2 -IIS Service - CiSvc | Internet Information Service (IIS) Monitoring | |
| Edit | ZC-IIS2 -IIS Services - IISADMIN | Internet Information Service (IIS) Monitoring | |
| Edit | ZC-IIS2-IIS Monitor | IIS Monitor Set | |
| Edit | ZC-PS1-Print Server Monitor | It's used to check job Errors, Total job Printed,Total pages printed,ou... | |
| Edit | ZC-Server Reboot | Check the Status of Server Uptime. | |
| Edit | ZC-SQL2 - MSSQLSERVER Services - MSSQLSERVER | MSSQLSERVER Service | |
| Edit | ZC-SQL2-MS SQL Server Production | Monitors the Performance of the SQL Server | |
| Edit | ZC-SV1- 2000 Server Basic Services | checks windows service for every 3 Minutes & restarted if stopped. | |
| Edit | ZC-SV1- Windows Server 2000 Service - Computer Browser (browser) | Computer Browser (browser) | |
| Edit | ZC-SV1- Windows Server 2000 Service - Cryptographic Services (Cryptsvc) | Cryptographic Services (Cryptsvc) | |
| Edit | ZC-SV1- Windows Server 2000 Service - Dhcp | DHCP Client | |
| Edit | ZC-SV1- Windows Server 2000 Service - dmserver | Logical Disk Manager - dmserver | |
| Edit | ZC-SV1- Windows Server 2000 Service - Dnscache | DNS Service for clients. | |

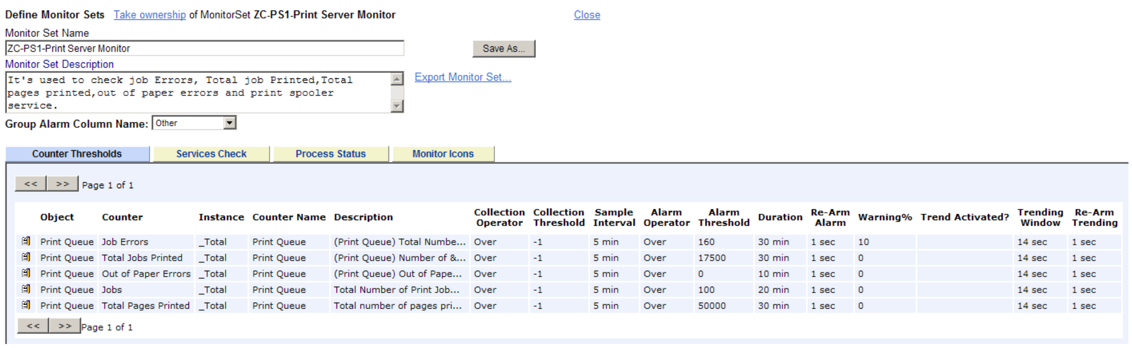
<< >> Add Import Page 3 of 6

3. A página **Definir conjuntos de monitores** será exibida. A guia **Limites do contador** é inicialmente exibida, que é a guia que desejamos rever. Esta vista da planilha exibe as configurações

definidas para cada um dos contadores. Se você deseja editar um contador, clique no ícone de edição na coluna mais a esquerda para exibir o assistente de edição para aquele contador.

> **Nota:** Você pode editar uma amostra de conjuntos de monitores ZC, mas essa amostra poderá ser substituída se o recurso de atualização estiver ativado em Sistema > Configurar. Caso deseje personalizar uma amostra de conjuntos de monitores ZC e assegurar que suas alterações sejam preservadas, crie uma cópia da amostra do conjunto de monitores ZC e faça as alterações na cópia.

Nós desejamos rever as configurações de todos os contadores neste conjunto de monitores, portanto, vamos permanecer com a vista da planilha.




| | Object | Counter | Instance | Counter Name | Description | Collection Operator | Collection Threshold | Sample Interval | Alarm Operator | Alarm Threshold | Duration | Re-Arm Alarm | Warning% | Trend Activated? | Trending Window | Re-Arm Trending |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Print Queue | Job Errors | _Total | Print Queue | (Print Queue) Total Numbe... | Over | -1 | 5 min | Over | 160 | 30 min | 1 sec | 10 | | 14 sec | 1 sec |
| | Print Queue | Total Jobs Printed | _Total | Print Queue | (Print Queue) Number of &... | Over | -1 | 5 min | Over | 17500 | 30 min | 1 sec | 0 | | 14 sec | 1 sec |
| | Print Queue | Out of Paper Errors | _Total | Print Queue | (Print Queue) Out of Pape... | Over | -1 | 5 min | Over | 0 | 10 min | 1 sec | 0 | | 14 sec | 1 sec |
| | Print Queue | Jobs | _Total | Print Queue | Total Number of Print Job... | Over | -1 | 5 min | Over | 100 | 20 min | 1 sec | 0 | | 14 sec | 1 sec |
| | Print Queue | Total Pages Printed | _Total | Print Queue | Total number of pages pri... | Over | -1 | 5 min | Over | 50000 | 30 min | 1 sec | 0 | | 14 sec | 1 sec |

4. Vamos examinar as primeiras cinco colunas da guia **Limites do contador** para este conjunto de monitores.

   Neste caso, todos os contadores se referem ao mesmo objeto `Print Queue`. Os conjuntos de monitores não são limitados a um único objeto de desempenho, mas tem sentido agrupar logicamente os contadores em um único conjunto de monitores em torno de uma determinada função do Windows.

   A coluna **Instância** é na verdade uma subcategoria do objeto, não o contador. Os contadores são definidos para uma combinação de objeto e instância. Por exemplo, as instâncias do objeto `Print Queue` são os nomes de impressoras específicas nas quais a máquina de destino pode imprimir, juntamente com a instância denominada `_Total`.

   A instância `_Total` combina os valores numéricos de quaisquer dados de contador provenientes de todas as impressoras e soma esses valores. Mas ela também age como um tipo de "instância de cartão coringa". Sem a instância `_Total`, é necessário especificar cada instância usando um nome exato de impressora, o que dificulta a aplicação do mesmo conjunto de monitores a várias máquinas. O verdadeiro benefício da instância `_Total` neste caso está na capacidade de determinar se existem *erros de impressora em qualquer impressora*. Quando você souber isso, poderá investigar o motivo específico.

| Object | Counter | Instance | Counter Name | Description |
|---|---|---|---|---|
| Print Queue | Job Errors | _Total | Print Queue | (Print Queue) Total Numbe... |
| Print Queue | Total Jobs Printed | _Total | Print Queue | (Print Queue) Number of &... |
| Print Queue | Out of Paper Errors | _Total | Print Queue | (Print Queue) Out of Pape... |
| Print Queue | Jobs | _Total | Print Queue | Total Number of Print Job... |
| Print Queue | Total Pages Printed | _Total | Print Queue | Total number of pages pri... |

5. O próximo conjunto de colunas descreve as configurações da coleção e dos limites de alarme. Observe que os valores **Operador de coleta** e **Limite de coleta** estão definidos como `Over -1`. O critério de coleta `Over -1` é usado com frequência para garantir que qualquer valor, incluindo zero, seja coletado, independentemente de um limite de alarme ser ou não atingido. Isso assegura que você possa rever todos os dados gerados por um contador.

   Cada contador fornece um novo valor a cada cinco minutos, como especificado pela coluna **Intervalo de amostra**.

Valores altos de **Limite do alarme** são definidos para os contadores `Total Jobs Printed` e `Total Pages Printed`. Isso é apropriado porque uma impressora de alto volume de irá alcançar com facilidade esta quantidade de trabalhos de impressão e de páginas impressas.

O valor de **Limite do alarme** para `Jobs` e `Job Errors` é muito menor. O contador `Jobs` retorna o número de trabalhos atualmente em processamento e, portanto, espera-se que ele seja pequeno. O contador `Job Errors` retorna o número de erros de trabalho que ocorreram desde a última inicialização do servidor de impressão. Um impressora de alto volume irá exceder rapidamente este limite de alarme se houver um problema com a impressora.

O contador `Out of Paper Errors` mostra um limite de zero, que é o valor normal quando não ocorreram erros de falta de papel desde a última inicialização do servidor de impressão. Mesmo que um único erro de "falta de papel" ocorra, *qualquer* valor `Over 0` acionará uma condição de alerta, sinalizando que é preciso adicionar papel à impressora.

| Counter | | Collection Operator | Collection Threshold | Sample Interval | Alarm Operator | Alarm Threshold | Duration | Re-Arm Alarm |
|---|---|---|---|---|---|---|---|---|
| Job Errors | | Over | -1 | 5 min | Over | 160 | 30 min | 1 sec |
| Total Jobs Printed | | Over | -1 | 5 min | Over | 17500 | 30 min | 1 sec |
| Out of Paper Errors | | Over | -1 | 5 min | Over | 0 | 10 min | 1 sec |
| Jobs | | Over | -1 | 5 min | Over | 100 | 20 min | 1 sec |
| Total Pages Printed | | Over | -1 | 5 min | Over | 50000 | 30 min | 1 sec |

6. As cinco colunas finais especificam os alarmes de aviso e os alarmes de tendência. O alarme de aviso é especificado como um percentual. Para o contador `Jobs Errors`, um alarme de aviso é acionado quando o valor do contador atinge 10% do seu limite de alarme.

   Um alarme de tendência, se ativado, calcula a linha de tendência com base nos dados coletados. Se a linha de tendência determina que o limite do alarme será excedido dentro do período de tempo da **Janela de tendência** , um alarme de tendência é acionado.

   A não ser que o recursos seja crítico, ou já está sob investigação, os alarmes de aviso e alarmes de tendência não são geralmente usados. Normalmente, uma janela de tendências deve ser definida para o tempo que você precisa para se preparar para uma condição de alerta, caso ocorra.

   Os alarmes com status de aviso e de tendência não criam entradas no registro de alarmes, mas alteram a imagem do ícone Alarme em várias janelas de exibição. É possível gerar um relatório de alarmes de tendência em Centro de informações > Emissão de relatórios > Relatórios > Monitor.

| Counter | | Warning% | Trend Activated? | Trending Window | Re-Arm Trending |
|---|---|---|---|---|---|
| Job Errors | | 10 | | 14 sec | 1 sec |
| Total Jobs Printed | | 0 | | 14 sec | 1 sec |
| Out of Paper Errors | | 0 | | 14 sec | 1 sec |
| Jobs | | 0 | | 14 sec | 1 sec |
| Total Pages Printed | | 0 | | 14 sec | 1 sec |

# Atribuindo conjuntos de monitores

Você atribui conjuntos de monitores em Monitor > **Atribuir monitoramento** a IDs de máquinas específicas. Você tem a opção de personalizar os conjuntos de monitores aplicados de duas formas:

- Conjuntos de Monitores Individualizados
- Auto-Aprendizado

# Conjuntos de Monitores Individualizados

É possível *individualizar* as configurações do conjunto de monitores a uma máquina.

1. Em Monitor > **Atribuir monitoramento**, selecione um conjunto de monitores *padrão* utilizando a lista suspensa <Select Monitor Set>.
2. Atribua esse conjunto de monitores padrão a uma ID de máquina. O nome do conjunto de monitores será exibido na coluna **Conjunto de Monitores**.
3. Clique no ícone do conjunto de monitores individualizado na coluna **Conjunto de Monitores** para exibir as mesmas opções exibidas durante a definição de um conjunto de monitores padrão. *Um conjunto de monitores individualizado adiciona o prefixo (IND) ao seu nome.*
4. Opcionalmente, altere o nome ou descrição do conjunto de monitores individualizado, depois clique no botão **Salvar**. Fornecer nome e descrição exclusivos ajuda a identificar um conjunto de monitores individualizado nos relatórios e arquivos de registro.
5. Faça as alterações nas configurações do monitoramento do conjunto de monitores individualizado e clique no botão **Confirmar**. As alterações se aplicam apenas à maquina individual à qual o monitor individualizado está atribuído.

> **Nota:** As alterações de um conjunto de monitores padrão não têm efeito sobre os conjuntos de monitores individualizados copiados dele.

# Autoaprendizado dos Conjuntos de monitores

É possível ativar limites de alarme do **Autoaprendizado** para qualquer conjunto de monitores padrão atribuído às IDs de máquina selecionadas. Isso ajusta automaticamente os limites de alarme baseados nos dados de desempenho atual por máquina.

Cada máquina atribuída coleta dados de desempenho durante um período especificado. Durante esse período, nenhum alarme é acionado. Ao final da sessão de autoaprendizado, o limite do alarme de cada máquina atribuída é ajustado automaticamente de acordo com o desempenho real da máquina. Você pode ajustar manualmente os valores do limite de alarme calculados pelo **Autoaprendizado** ou executar outra sessão de **Autoaprendizado**. O **Autoaprendizado** não pode ser usado com conjuntos de monitores individualizados.

# Conjuntos SNMP

Determinados dispositivos de rede como impressoras, roteadores, firewalls, servidores e dispositivos UPS não suportam a instalação de um agente. Mas um agente do VSA instalado em uma máquina gerenciada na mesma rede que o dispositivo pode ler ou gravar naquele dispositivo usando o **protocolo SNMP.** .

# Monitoramento SNMP básico

A maneira mais rápida de começar a aprender a usar o VSA para monitorar dispositivos SNMP é atribuir um "conjunto SNMP" predefinido a um dispositivo e ver os resultados. Quando você perceber como a configuração básica é simples, poderá analisar recursos SNMP mais avançados.

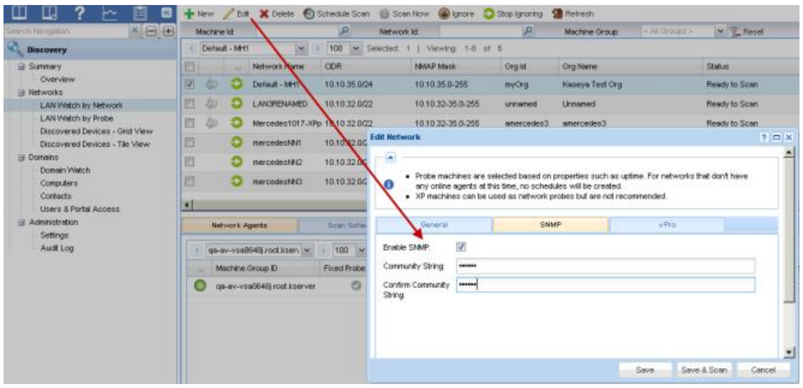
O monitoramento de dispositivos habilitados para SNMP pode ser iniciado em três etapas:

1. Detecte dispositivos SNMP usando Discovery > **LAN Watch** *(página 19)*.
2. Atribua conjuntos SNMP predefinidos aos dispositivos detectados em Monitor > **Atribuir SNMP** *(página 19)*.
3. Exiba alarmes SNMP usando Monitor > **Log SNMP** *(página 21)*

# LAN Watch e SNMP

O recurso **LAN Watch por rede** ou **LAN Watch por verificação** no módulo **Discovery** usa um agente do VSA existente em uma máquina gerenciada para verificar periodicamente a rede local em busca de quaisquer novos dispositivos conectados a essa LAN desde a última execução de LAN Watch.

*A máquina de detecção de LAN Watch emite as solicitações SNMP aos dispositivos SNMP que detecta na mesma LAN.* Portanto, você deve executar LAN Watch *primeiro* para ter acesso a dispositivos habilitados para SNMP usando o VSA.




Para incluir dispositivos SNMP na varredura de detecção realizada por LAN Watch:

1. Selecione um ID de máquina na mesma LAN que os dispositivos SNMP que você deseja detectar.
2. Selecione a caixa de seleção **Ativar SNMP**.
3. Insira um `community name` nos campos **Ler nome da comunidade** e **Confirmar**.

   Um nome de comunidade é uma credencial para obter acesso a um dispositivo habilitado para SNMP. O nome padrão da comunidade de "leitura" é geralmente `public`, em letras minúsculas, mas cada dispositivo pode ser configurado de maneira diferente. Talvez você precise identificar ou redefinir o nome da comunidade no dispositivo diretamente caso não tenha certeza do nome a usar.
4. Clique no botão **Agendar e fazer varredura** na parte inferior da página **Editar rede**. Isto iniciará a varredura imediatamente.
5. Analise os dispositivos detectados habilitados para SNMP na página Monitor > **Atribuir SNMP** *(página 19)*.

# Atribuir SNPM

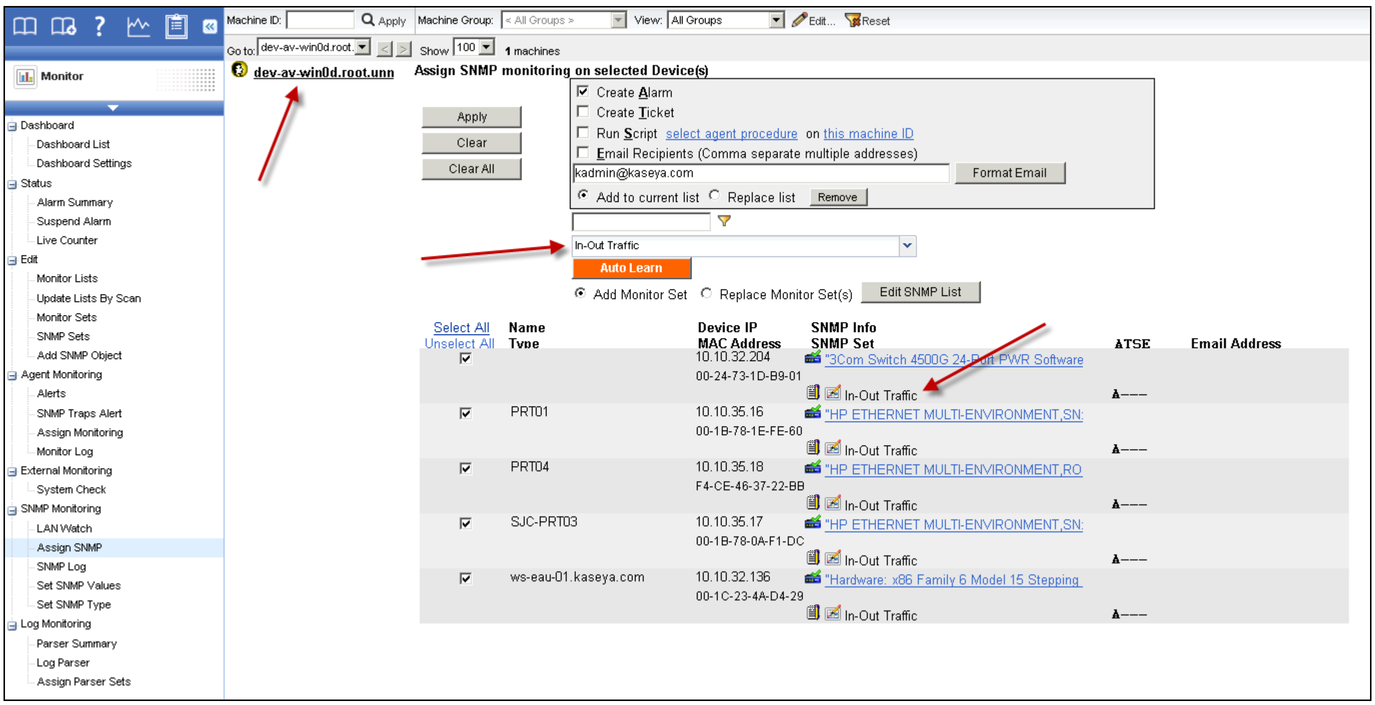
Dispositivos SNMP só são exibidos na página Monitor > **Atribuir SNMP** *após* a execução do **LAN Watch** *(página 19)* na máquina de detecção.

Para atribuir o monitoramento de um dispositivo habilitado para SNMP usando a página **Atribuir SNMP**:

1. Selecione a máquina de detecção no lado esquerdo da página. Isso exibe todos os dispositivos habilitados para SNMP na mesma LAN.
2. Selecione um conjunto SNMP na lista suspensa.

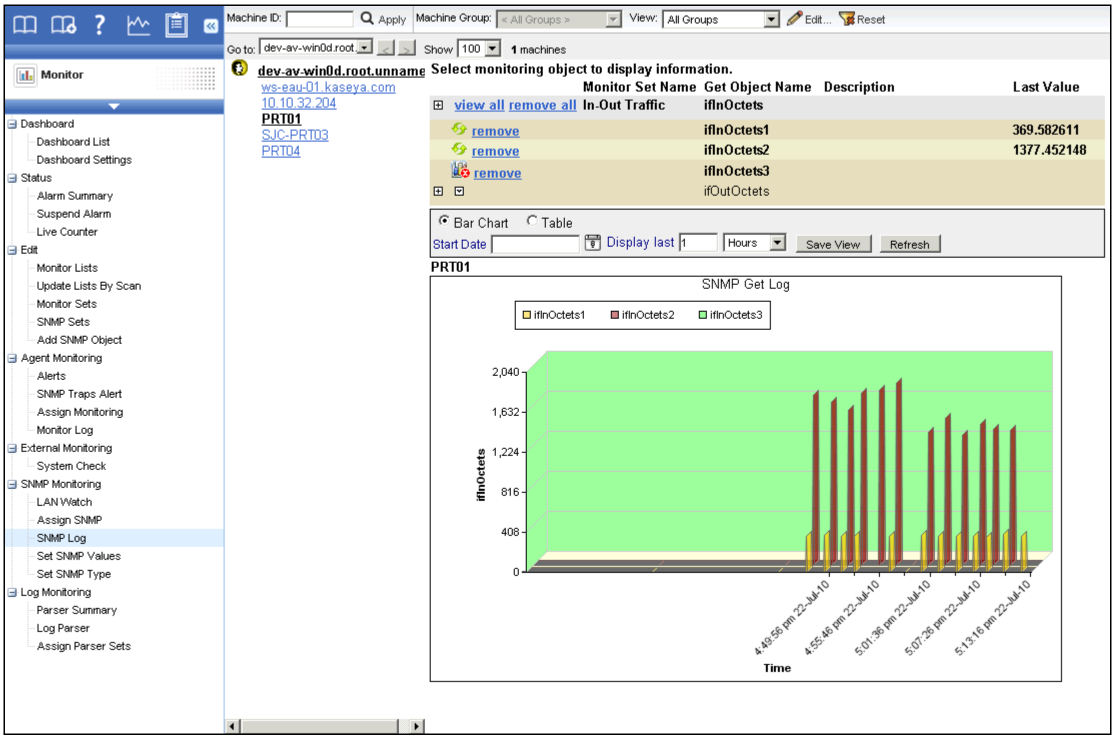
> **Nota:** Se nenhum conjunto SNMP aparecer na lista suspensa, acesse a página **Conjuntos SNMP**, selecione um conjunto SNMP e depois clique no botão **Salvar como** para fazer uma cópia desse conjunto. Para fins de teste, faça uma cópia de um conjunto SNMP que seja semelhante ao dispositivo que você deseja monitorar. Por exemplo, se quiser monitorar um roteador, faça uma cópia de um conjunto SNMP para roteadores. Se quiser monitorar uma impressora, faça uma cópia de um conjunto SNMP para impressoras, e assim por diante. Ao usar um conjunto SNMP pela primeira vez, você não precisa se preocupar se alguns dos objetos nesse conjunto não se aplicar ao dispositivo que você deseja monitorar. É possível **editar sua cópia de um conjunto SNMP** *(página 23)* a qualquer momento antes ou depois de atribuí-la a uma máquina.

3. Selecione um ou mais dispositivos detectados habilitados para SNMP.
4. Clique no botão **Aplicar**.
5. Aguarde cerca de 15 minutos até que os dispositivos habilitados para SNMP retornem dados de monitoramento SNMP ao VSA. Em seguida, exiba os resultados do monitoramento na página **Log SNMP** *(página 21)*.



# Registro SNMP

A página SNMP **Log SNMP** mostra os resultados de dispositivos SNMP monitorados, em formato de gráfico ou tabela, depois de eles terem sido atribuídos a um dispositivo usando o recurso **Atribuir SNMP** *(página 19)*. É necessário aguardar cerca de 15 minutos para que os dados sejam exibidos na página após a atribuição do conjunto SNMP ao dispositivo. Alguns objetos no conjunto SNMP talvez não retornem dados. A ausência de dados retornados pode ocorrer quando um determinado objeto no conjunto SNMP não se aplica ao dispositivo. Ou talvez o objeto seja correto para o dispositivo, mas não esteja ativo no momento. Navegue pelos vários objetos no conjunto SNMP dessa página até encontrar um objeto que esteja retornando dados. Familiarize-se com os métodos de alteração da exibição dos dados usando os vários controles.




Para selecionar os dados a serem exibidos:

1. Clique em um link de ID de máquina para listar todos os dispositivos SNMP associados a essa ID de máquina.
2. Clique no endereço IP ou no nome de um dispositivo SNMP para exibir todos os conjuntos SNMP e objetos MIB atribuídos ao dispositivo SNMP.
3. Clique no ícone Expandir ⊞ para exibir as configurações de coleta e limites de um objeto MIB.
4. Clique no ícone da seta para baixo ⊡ para exibir dados de registro do objeto MIB nos formatos de gráfico ou tabela.
5. Clique na opção **Gráfico de Barras** ou **Tabela** para selecionar o formato de exibição dos dados de registro.

Os objetos do monitor SNMP podem conter várias instâncias e serem visualizados juntos em um gráfico ou tabela. Por exemplo, um comutador de rede pode ter 12 portas. Cada uma é uma instância e pode conter dados de registro. Todas as 12 instâncias podem ser combinadas em um gráfico ou tabela. Os gráficos de barras SNMP são em formato 3D para permitir a visualização de várias instâncias.

# Conceitos sobre SNMP

Antes de tentar editar um conjunto SNMP, você deve se familiarizar com os seguintes conceitos sobre SNMP.

## Três tipos de mensagens SNMP

O VSA é compatível com três tipos de mensagens SNMP.

1. **Mensagens Get de "leitura"**: o dispositivo habilitado para SNMP responde a uma solicitação "get" SNMP proveniente do software de gerenciamento SNMP, como um agente do VSA em uma máquina. *A maioria das funções SNMP no VSA, incluindo Conjuntos SNMP, envolve mensagens Get.*
2. **Mensagens Set de "gravação"**: softwares de gerenciamento SNMP, como o VSA, gravam um valor no objeto MIB de um dispositivo habilitado para SNMP. Isso pode ser feito para fins de referência ou para alterar o comportamento do dispositivo. Uma página do VSA executa mensagens do conjunto SNMP: **Definir valores SNPM**.
3. **Mensagens Trap de "escuta"**: mensagens enviadas por um dispositivo habilitado para SNMP a um agente de "escuta", sem que elas tenham sido solicitadas, com base em algum evento que esse dispositivo detectou. Uma página do VSA configura e responde a mensagens de interceptações SNMP: **Alerta de interceptações SNMP** (página 30).

## Objetos MIB

A edição dos conjuntos SNMP usados pelo VSA para monitorar dispositivos SNMP requer uma compreensão básica de objetos MIB e arquivos MIB. Caso você já esteja familiarizado com esses conceitos, vá para **Como editar conjuntos SNMP** *(página 23)*.

Cada dispositivo habilitado para SNMP responde apenas a um conjunto específico de solicitações SNMP. Cada solicitação SNMP é identificada exclusivamente por uma ID de objeto, ou **OID**. Por exemplo, uma OID denominada `ifInOctets` é representada pela OID numérica `.1.3.6.1.2.1.2.2.1.10`. A OID baseada em caracteres correspondente para `ifInOctets` é `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets`.

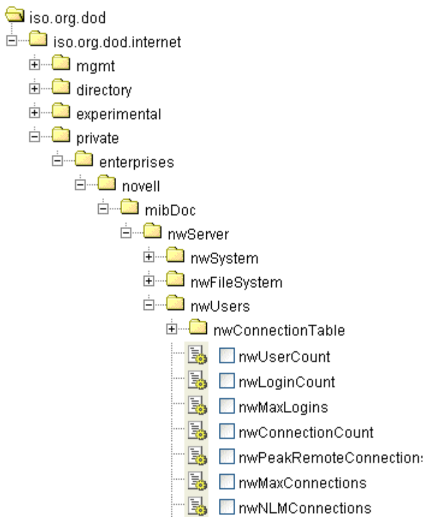
Cada fabricante de dispositivos publica as OIDs com suporte pelos dispositivos habilitados para SNMP que fabricam no formato de um **arquivo MIB**. Portanto, OIDs são geralmente chamadas de **objetos MIB**. Os arquivos MIB podem ser importados para um aplicativo de gerenciamento de MIB, como o VSA. O VSA vem pré-instalado com vários objetos MIB populares e, por isso, a importação de objetos MIB é geralmente necessária apenas para dispositivos com objetos MIB especializados.

No VSA, objetos MIB são combinados para criar um **conjunto SNMP**. Após a realização de LAN Watch, são atribuídos conjuntos SNMP a um dispositivo habilitado para SNMP na mesma LAN e usados para monitorar o desempenho desse dispositivo.

### Árvore MIB

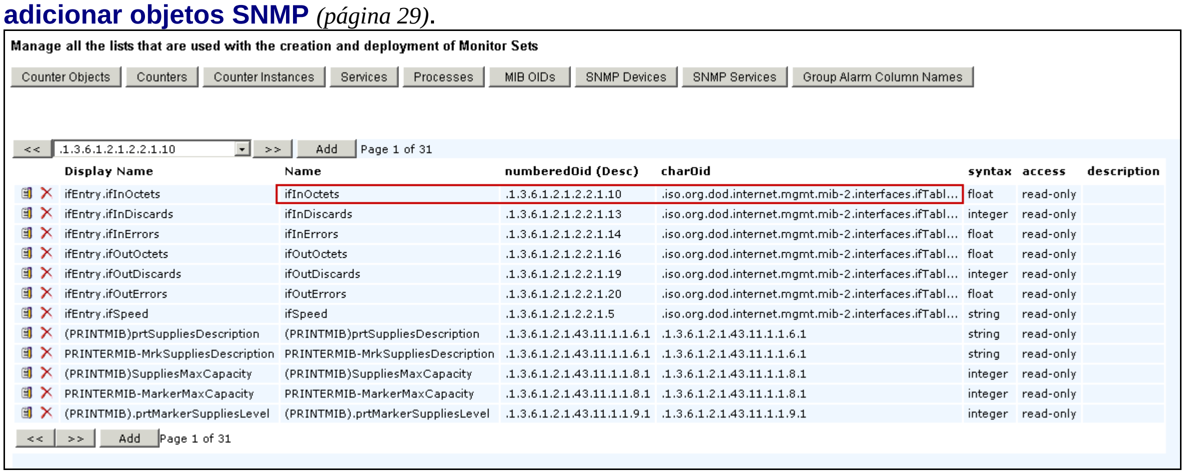
Os fabricantes tentam padronizar a identificação de objetos MIB que eles utilizam em dispositivos organizando-os em uma Árvore MIB. Por exemplo, roteadores podem usar muitos dos mesmos objetos MIB e ter apenas alguns poucos objetos MIB especializados diferentes para dar suporte ao seu produto específico.

Você pode usar a OID numérica ou a OID baseada em caracteres para localizar a posição do objeto MIB na árvore. Veja a seguir um exemplo de uma árvore MIB baseada em caracteres.




### Objetos MIB na página Listas de monitores

No VSA, é possível ver uma lista de todos os objetos MIB atualmente disponíveis para inclusão em um conjunto SNMP. Selecione a página Monitor > **Listas de monitores** e clique no botão **OIDs MIB** para ver uma tabela semelhante à exibida abaixo. Você pode adicionar objetos MIB à lista importando arquivos MIB ao VSA para dar suporte a um dispositivo habilitado para SNMP específico. Consulte **Como adicionar objetos SNMP** *(página 29)*.



Manage all the lists that are used with the creation and deployment of Monitor Sets

Counter Objects | Counters | Counter Instances | Services | Processes | MIB OIDs | SNMP Devices | SNMP Services | Group Alarm Column Names

<< .1.3.6.1.2.1.2.2.1.10 >> Add Page 1 of 31

| Display Name | Name | numberedOid (Desc) | charOid | syntax | access | description |
|---|---|---|---|---|---|---|
| ifEntry.ifInOctets | ifInOctets | .1.3.6.1.2.1.2.2.1.10 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | float | read-only | |
| ifEntry.ifInDiscards | ifInDiscards | .1.3.6.1.2.1.2.2.1.13 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | integer | read-only | |
| ifEntry.ifInErrors | ifInErrors | .1.3.6.1.2.1.2.2.1.14 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | float | read-only | |
| ifEntry.ifOutOctets | ifOutOctets | .1.3.6.1.2.1.2.2.1.16 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | float | read-only | |
| ifEntry.ifOutDiscards | ifOutDiscards | .1.3.6.1.2.1.2.2.1.19 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | integer | read-only | |
| ifEntry.ifOutErrors | ifOutErrors | .1.3.6.1.2.1.2.2.1.20 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | float | read-only | |
| ifEntry.ifSpeed | ifSpeed | .1.3.6.1.2.1.2.2.1.5 | .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTabl... | string | read-only | |
| (PRINTMIB)prtSuppliesDescription | (PRINTMIB)prtSuppliesDescription | .1.3.6.1.2.1.43.11.1.1.6.1 | .1.3.6.1.2.1.43.11.1.1.6.1 | string | read-only | |
| PRINTERMIB-MrkSuppliesDescription | PRINTERMIB-MrkSuppliesDescription | .1.3.6.1.2.1.43.11.1.1.6.1 | .1.3.6.1.2.1.43.11.1.1.6.1 | string | read-only | |
| (PRINTMIB)SuppliesMaxCapacity | (PRINTMIB)SuppliesMaxCapacity | .1.3.6.1.2.1.43.11.1.1.8.1 | .1.3.6.1.2.1.43.11.1.1.8.1 | integer | read-only | |
| PRINTERMIB-MarkerMaxCapacity | PRINTERMIB-MarkerMaxCapacity | .1.3.6.1.2.1.43.11.1.1.8.1 | .1.3.6.1.2.1.43.11.1.1.8.1 | integer | read-only | |
| (PRINTMIB).prtMarkerSuppliesLevel | (PRINTMIB).prtMarkerSuppliesLevel | .1.3.6.1.2.1.43.11.1.1.9.1 | .1.3.6.1.2.1.43.11.1.1.9.1 | integer | read-only | |

<< >> Add Page 1 of 31

# Como editar conjuntos SNMP

## Conjuntos SNMP - Parte 1

No VSA, selecione Monitor > **Conjuntos SNMP** e, em seguida, selecione uma determinada amostra de conjunto SNMP para ver uma exibição de colunas em tabela semelhante à da imagem abaixo.

Esse exemplo de conjunto SNMP mostra um par de objetos MIB pertencentes ao objeto MIB principal chamado `IFEntry.`. Objetos `IFEntry` monitoram o fluxo de dados de entrada e saída de um dispositivo, como um cabo conectado à porta de um comutador. Em termos de TCP/IP, esse ponto no fluxo de dados é conhecido como a *interface* do dispositivo e, portanto, `IFEntry` significa a "entrada da interface". O objeto MIB `ifInOctets` se refere especificamente ao número de bytes de 8 bits, chamados de "octetos" nesse caso, que fluem em direção a uma única interface. O objeto MIB

ifOutOctets é o número de bytes de 8 bits que fluem para fora de uma única interface.

Usando apenas esses dois objetos MIB, você pode monitorar a taxa de dados de entrada e saída em uma conexão de rede e atribuir um limite de alarme caso esse fluxo de dados ultrapasse um determinado valor.

| MIBObject | SNMP Version | SNMP Instance | Data Type | Name | Description |
|---|---|---|---|---|---|
| ifEntry.ifInOctets | 1 | 1-3 | ratePerSecond | ifInOctets | |
| ifEntry.ifOutOctets | 1 | 1-3 | ratePerSecond | ifOutOctets | |

**MIBObject**: o identificador de objeto MIB se baseia nos dois últimos níveis de sua OID baseada em caracteres. Por exemplo, na primeira linha, a OID completa baseada em caracteres para esse objeto MIB é .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets. Portanto, a primeira coluna da tabela exibe ifEntry.ifInOctets.

**Versão SNMP**: o SNMP é um protocolo em evolução. Há suporte à versão 1 em todos os dispositivos e esta é o padrão. A versão 2c define mais atributos, como tipos de dados adicionais, e criptografa os pacotes para o agente SNMP e a partir do agente SNMP. *Apenas selecione a versão 2c se você souber que o dispositivo é compatível com essa versão.*

**Instância SNMP**: pode haver várias instâncias de um objeto MIB em um único dispositivo. Por exemplo, um comutador tem várias portas. Você pode especificar o intervalo de instâncias em um dispositivo que deseja monitorar, como 1-5,6 ou 1,3,7. Se houver apenas uma instância de um objeto MIB no dispositivo, especifique 0 ou deixe-a em branco.

**Valor retornado como**: se o objeto MIB retornar um valor numérico, você poderá optar por retornar esse valor como um **Total** ou uma **Taxa por segundo**. Em geral, para o monitoramento da interface, é preferível conhecer a taxa de dados transmitidos para dentro e fora de uma porta. Portanto, IfInOctets e IfOutOctets são definidos para Taxa por segundo. Objetos MIB que retornam uma sequência em vez de um número não exibem esse campo extra em Conjuntos SNMP.

**Nome e descrição**: estes são os identificadores "amigáveis" para um objeto MIB. Você pode alterar seus padrões na página Monitor > **Lista de monitores** ou em um conjunto SNMP.

# Conjuntos SNMP - Parte 2

O próximo conjunto de colunas na exibição em tabela especifica o *limite de coleta* e o *limite de alarme* para os valores retornados pelo dispositivo ao VSA.

| Name | Collection Operator | Collection Threshold | SNMP Timeout | Alarm Operator | Alarm Threshold | Duration | Re-Arm Alarm |
|---|---|---|---|---|---|---|---|
| ifInOctets | Over | -1 | 2 sec | Over | 1000000 | 30 sec | 1 days |
| ifOutOctets | Over | -1 | 2 sec | Over | 1000000 | 30 sec | 1 days |

## Coleção

Minimize a coleta de dados de log no VSA usando um limite de coleta que apenas retorne dados quando isso for importante para você. Se quiser tudo, e o **Operador de coleta** for Over, defina o **Limite de coleta** como -1, o que significa tudo acima de -1.

- **Operador de coleta**: para valores de retorno de sequência de caracteres, as opções são Changed, Equal ou NotEqual para o **Limite de coleta**. Para valores de retorno numéricos, as opções são Equal, NotEqual, Over ou Under para o **Limite de coleta**.
- **Tempo Limite SNMP** - Especifica quanto tempo o agente aguarda por uma resposta do dispositivo SNMP antes de desistir. O padrão é dois segundos.

### Alarmes

Especifique quando uma condição de alerta ocorre. Isso não significa que um alarme será necessariamente acionado. O acionamento de um alarme para uma condição de alerta é decidido quando o conjunto SNMP é atribuído a um dispositivo.

- **Operador de alarme**: para valores de retorno de sequência de caracteres, as opções são `Changed`, `Equal` ou `NotEqual` para o **Limite de alarme**. Para valores numéricos de retorno, as opções são `Equal`, `NotEqual`, `Over` `Under` ou `Percent Of`. A seleção da opção `Percent Of` exibe um novo campo **Porcentagem do objeto**. O campo **Porcentagem do objeto** serve como um ponto de referência de 100% para fins de comparação.
- **Duração**: especifique por quanto tempo os valores retornados devem exceder continuamente o limite de alarme para gerar a condição de alerta. Muitas condições de alerta executam o alarme somente se o nível for sustentado ao longo do período.
- **Rearmar alarme**: suprime condições de alerta adicionais desse mesmo problema nesse período. Isto reduz a confusão de muitas condições de alertas para a mesma emissão.

## Conjuntos SNMP - Parte 3

As últimas colunas na exibição em tabela de um conjunto SNMP definem o endereço a ser notificado *antes* da ocorrência de uma condição de alerta. Elas são utilizadas com menos frequência em comparação às colunas anteriores.

**Alarmes de aviso** e **alarmes de tendência** não criam entradas de alarme no log de alarmes, mas alteram a imagem do ícone de alarme em várias janelas de exibição. Você pode gerar um relatório de alarme de tendência em Relatórios > Monitor.

| Name | Warning% | Trend Activated? | Trending Window | Re-Arm Trending |
|---|---|---|---|---|
| ifInOctets | 10 | No - Trending is not need... | 14 days | 1 days |
| ifOutOctets | 10 | No - Trending is not need... | 14 days | 1 days |

### Alarmes de aviso

- **% de aviso**: mostra opcionalmente uma *condição de alerta de aviso* quando o valor retornado está dentro de uma porcentagem especificada do **Limite de alarme**. Um ícone de aviso é exibido no lugar de um alarme.

### Alarmes de tendência

Alarmes de tendência utilizam dados históricos para prever quando a próxima condição de alerta ocorrerá.

- **Tendência ativada?**- Se afirmativo, uma linha de tendência de regressão linear será calculada de acordo com os últimos 2.500 pontos de dados registrados.
- **Janela Tendência** - O período usado para estender a linha de tendência calculada para o futuro. Se uma linha de tendência prevista excede o limite do alarme dentro do período futuro específico, uma condição de alerta de tendência é gerada. Normalmente, uma janela de tendências deve ser definida para o tempo que você precisa para se preparar para uma condição de alerta, caso ocorra.
- **Rearmar tendência**: suprime condições de alarme de tendências adicionais para esse mesmo problema durante esse período.

# Recursos SNMP avançados

A edição manual de um conjunto SNMP implica que você conhece os objetos MIB que devem ou não pertencer a um dispositivo, bem como os valores de limite de coleta e alarme que devem ser

atribuídos a ele. Mas, e se você não conhecer esses objetos e valores para um determinado dispositivo? Dois recursos avançados de detecção são fornecidos em Monitor > **Atribuir SNMP** *(página 19)* para ajudá-lo:

- **Conjuntos rápidos** (página 26): um comando "walk" limitado de SNMP é realizado em um dispositivo SNMP para detectar os objetos MIB atualmente utilizados no dispositivo. Você pode selecionar apenas os objetos MIB que têm valores e criar um "conjunto rápido" para começar a monitorar o dispositivo imediatamente. O valor mais recente é mostrado para cada objeto MIB quando você cria o conjunto rápido.
- **Autoaprendizado** (página 27): você pode usar o valor inicial exibido ao criar um conjunto rápido (ou os valores predefinidos em um conjunto SNMP padrão) e esperar que tudo funcione. Outra opção é ativar o Autoaprendizado para um conjunto rápido aplicado ou para um conjunto padrão e deixar que o agente de monitoramento calcule os limites apropriados para você. Por padrão, o ciclo de aprendizado é de uma hora. Durante esse tempo, a opção de Autoaprendizado determina o valor médio retornado por um objeto MIB em um dispositivo e define limites para condições de coleta e alerta. Se desejar, você pode alterar os critérios de autoaprendizado ou pode modificar os cálculos resultantes após a conclusão do ciclo de autoaprendizado.

A seção **Recursos SNMP avançados** também discute o seguinte:

- **Conjuntos SNMP individualizados** (página 28) - São conjuntos SNMP padrão aplicados a um dispositivo individual e personalizados manualmente.
- **Tipos SNMP** (página 29) - É o método de atribuição automática de conjuntos SNMP padrão aos dispositivos, de acordo com o **tipo SNMP** *(página 29)* determinado durante um LAN Watch.
- **Como adicionar objetos SNMP** (página 29): adicione objetos MIB ao VSA para um conjunto SNMP se ainda não estiverem disponíveis.
- **Interceptações SNMP** (página 30): configura alertas para uma máquina gerenciada que atua como "ouvinte" de interceptações SNMP ao detectar uma mensagem de **interceptação SNMP**.

# Configurações rápidas de SNMP

A página do link **Informações do SNMP** exibe uma lista de objetos MIB fornecidos pelo dispositivo SNMP específico que você selecionou. Estes objetos MIB são detectados ao realizar um comando "walk" limitado de SNMP em todos os dispositivos SNMP detectados sempre que um **LAN Watch** *(http://help.kaseya.com/webhelp/PTB/KDIS/R8/index.asp#1944.htm)* é executado. Você pode usar uma lista de objetos MIC detectados para criar instantaneamente um conjunto SNMP específico de dispositivos — chamado **conjunto rápido** — e aplicá-lo ao dispositivo. Após a criação, os conjuntos rápidos são iguais a qualquer conjunto padrão. Eles são exibidos em sua pasta privada em Monitor > **Conjuntos SNMP** e na lista suspensa em Monitor > **Atribuir SNMP**. Um `(QS)` prefixo mostra a você como o conjunto rápido foi criado. Como qualquer outro conjunto padrão, os conjuntos rápidos podem ser *individualizados* para um único dispositivo, usado com **Autoaprendizado** *(página 27)*, compartilhado com outros usuários e aplicado a dispositivos similares por todo o VSA.

1. Detecte dispositivos SNMP em Monitor > **LAN Watch** *(http://help.kaseya.com/webhelp/PTB/KDIS/R8/index.asp#1944.htm)*.
2. Atribua conjuntos SNMP para dispositivos detectados em Monitor > Atribuir SNMP.
3. Clique no hyperlink sob o nome do dispositivo, denominado link de Informações SNMP, na página **Atribuir SNMP** para exibir um diálogo.
   - Clique em **Objetos MIB detectados** e selecione um ou mais objetos MIB que foram detectados no dispositivo SNMP que você acabou de selecionar.
   - Clique em **Itens de conjuntos rápidos** e, se necessário, edite os limites dos alarmes para os objetos MIB selecionados.
   - Insira um nome após o prefixo **(QS)** no cabeçalho do diálogo.
   - Clique no botão **Aplicar** para aplicar o conjunto rápido ao dispositivo.
4. Exiba os dados de monitoramento SNMP retornados pelo conjunto rápido utilizando Monitor > Log SNMP, do mesmo modo que faria para qualquer outro conjunto SNMP padrão.

5. Mantenha, opcionalmente, o seu novo conjunto rápido utilizando Monitor > Conjuntos SNMP.

Use estas guias na página **Link para informações sobre SNMP** para configurar um conjunto rápido de SNMP.

### Guia Objetos MIB localizados

A guia **Objetos MIB Descobertos** lista todos os conjuntos de objetos descobertos pela última atividade SNMP que se aplicar ao dispositivo SNMP selecionado. Você pode usar essa guia para adicionar objetos e instâncias a um conjunto rápido SNMP para esse dispositivo.

- **Adicionar Instância** - Clique para adicionar essa instância desse objeto a uma "definição rápida" de exibição SNMP na mesma guia **Conjunto SNMP** dessa janela.
- **Adicionar Todas as Instâncias** - Clique para adicionar todas as instâncias desse objeto a uma "definição rápida" de exibição SNMP na mesma guia **Conjunto SNMP** dessa janela.
- **Objeto SNMP** - Nome do objeto SNMP. Se nenhum nome for fornecido para o objeto, a designação numérica OID será exibida.
- **Instância** - A instância do objeto. Muitos objetos têm várias instâncias, cada uma com um valor diferente. Por exemplo, as instâncias diferentes podem ser portas em um roteador ou bandejas para papel em uma impressora. O campo estará em branco se o último número de um OID for zero, que indica que só pode haver um membro desse objeto. Se uma instância não estiver em branco ou se houver um número que não seja 0, mais de uma "instância" desse mesmo objeto existirá para o dispositivo. É possível especificar o monitoramento de diversas instâncias de um objeto ao inserir um intervalo de números, como `1-5,6` ou `1,3,7`. Você também pode inserir `All`.
- **Valor SNMP Atual** - O valor retornado pela combinação objeto/instância pela última atividade SNMP.

### Guia Itens de Configuração Rápida

A guia **Itens de Configuração Rápida** configura os objetos e instâncias selecionados para inclusão em sua configuração SNMP rápida. Clique no ícone Editar para definir os atributos do monitoramento SNMP para os objetos selecionados. Você também pode usar o botão **Adicionar** para adicionar um novo objeto e definir esses mesmos atributos.

- **Objeto SNMP** - Nome do objeto SNMP ou número OID.
- **Instância SNMP** - O último número de uma ID de objeto pode ser expressa em uma tabela de valores em vez de em um único valor. Se a instância for um valor único, insira `0`. Se a instância for uma tabela de valores, insira um intervalo de números, como `1-5,6` ou `1,3,7`. Você também pode inserir `All`.
- **Operador de alarmes**: para valores de retorno de sequência de caracteres `Changed`, `Equal` ou `NotEqual`. Para valores numéricos de retorno, as opções são `Equal`, `NotEqual`, `Over` ou `Under.`
- **Limite de Alarme** - Defina um valor fixo com o qual o valor retornado será comparado, usando o **Operador de Alarme** selecionado, para determinar quando um alarme será acionado.
- **Valor Retornado como** - Se o objeto MIB retornar um valor numérico, você pode optar por retornar esse valor como um **Total** ou uma **Taxa Por Segundo**.
- **Valor SNMP Atual** - O valor retornado pela combinação objeto/instância pela última atividade SNMP.

## Autoaprendizado de conjuntos SNMP

Você pode habilitar limites do alarme de **Autoaprendizado** para qualquer conjunto DNMP padrão ou conjunto rápido que você atribui para dispositivos SNMP selecionados. Isso ajusta automaticamente os limites de alarme baseados nos dados de desempenho atual por dispositivo SNMP.

Cada dispositivo SNMP atribuído gerará dados de desempenho durante um período especificado. Durante esse período, nenhum alarme é acionado. Ao final da sessão de **Autoaprendizado**, o limite do alarme de cada dispositivo SNMP atribuído é ajustado automaticamente de acordo com o

desempenho real do dispositivo SNMP. Você pode ajustar manualmente os valores do limite de alarme calculados pelo **Autoaprendizado** ou executar outra sessão de **Autoaprendizado**. O **Autoaprendizado** não pode ser usado com conjuntos SNMP individualizados.

Para aplicar as configurações de **Autoaprendizado** aos dispositivos SNMP selecionados:

1. Selecione um conjunto SNMP *padrão* na lista suspensa `<Select SNMP Set>`. Ou clique no ícone de edição de um conjunto SNMP já atribuído para que um dispositivo preencha a lista suspensa `<Select SNMP Set>` com seu identificador.
2. Clique em **Autoaprendizado** para exibir a janela pop-up Autoaprendizado. Use um assistente para definir os parâmetros usados para calcular os valores de limite dos alarmes.
3. Atribua este conjunto SNMP padrão, modificado pelos seus parâmetros de **Autoaprendizado**, para selecionar dispositivos SNMP, se já não atribuídos.

Quando o **Autoaprendizado** for aplicado a uma ID de máquina e for executado no período especificado, você poderá clicar no ícone Substituir Autoaprendizado de um dispositivo SNMP específico e ajustar manualmente os valores de limite do alarme calculado. Também é possível executar novamente o **Autoaprendizado**, usando uma nova sessão dos dados de desempenho real para recalcular os valores de limite do alarme.

Use o procedimento a seguir para definir as configurações de auto-aprendizado SNMP na janela suspensa **Auto-aprendizado**.

Clique no ícone Editar para usar um assistente que o conduzirá nas três etapas requeridas para editar limites do alarme de autoaprendizado.

1. Habilite a opção **Autoaprendizado** para este objeto SNMP, caso apropriado, ao selecionar `Yes - Include`. Se `No - Do not include` for selecionado, nenhuma outra seleção neste assistente será aplicável.
   - **Período** - Insira o período em que os dados de desempenho serão coletados e usados para calcular limites de alarme automaticamente. Os alarmes não serão reportados durante esse período.
2. Exibe o **Objeto SNMP** do limite de alarme que está sendo modificado. Essa opção não pode ser alterada.
3. Insira os parâmetros do valor calculado.
   - **Computação** - Selecione um parâmetro do valor calculado. As opções incluem `MIN`, `MAX` ou `AVG`. Por exemplo, a seleção MÁX significa calcular o valor máximo coletado por um objeto SNMP durante o **Período** especificado acima.
   - **% de Aumento** - Adicione esse percentual ao valor **Computação** calculado acima, com o valor **Computação** representando 100%. O valor resultante representa o limite do alarme.
   - **Mínimo** - Defina um valor mínimo para o limite de alarme. O valor é calculado automaticamente como *dois desvios padrão abaixo* do valor **Computação** calculado, mas pode ser substituído manualmente.
   - **Máximo** - Defina um valor máximo para o limite de alarme. O valor é calculado automaticamente como *dois desvios padrão acima* do valor **Computação** calculado, mas pode ser substituído manualmente.

# Conjuntos SNMP Individualizados

É possível *individualizar* as configurações do conjunto SNMP a uma máquina.

1. Selecione um conjunto SNMP *padrão* na lista suspensa `<Select Monitor Set>`.
2. Atribua esse conjunto SNMP padrão a um dispositivo SNMP. O nome do conjunto SNMP será exibido na coluna **Informações sobre SNMP / Conjunto SNMP**.
3. Clique no ícone do conjunto de monitores individualizado na coluna **Informações sobre SNMP / Conjunto SNMP** para exibir as mesmas opções exibidas durante a definição de um conjunto SNMP padrão. *Um conjunto SNMP individualizado adiciona o prefixo (IND) ao nome do conjunto SNMP.*

4. Faça alterações ao seu novo conjunto SNMP individualizado. Essas alterações se aplicam apenas ao dispositivo SNMP individual ao qual está atribuído.

> **Nota:** *As alterações de um conjunto SNMP padrão não têm efeito sobre os conjuntos SNMP individualizados copiados dele.*

# Tipos SNMP

A maioria dos dispositivos SNMP é classificada como um certo tipo de dispositivo SNMP utilizando o objeto MIB `system.sysServices.0`. Por exemplo, alguns roteadores se identificam como roteadores genericamente ao retornar o valor `77` para o objeto MIB `system.sysServices.0`. Você pode utilizar o valor retornado pelo objeto MIB `system.sysServices.0` para atribuir automaticamente conjuntos SNMP para dispositivos, assim que eles são detectados por um LAN Watch.

> **Nota:** *O OID inteiro para* `system.sysServices.0` **é** `.1.3.6.1.2.1.1.7.0` **ou** `.iso.org.dod.internet.mgmt.mib-2.system.sysServices`.

Para atribuir conjuntos SNMP aos dispositivos *por tipo automaticamente*:

1. Adicione ou edite *tipos* de SNMP utilizando a guia **Dispositivo SNMP** em Monitor > Listas de monitores.
2. Adicione ou edite o valor retornado pelo objeto MIB `system.sysServices.0` *e associado com cada tipo SNMP* utilizando a guia **Serviços SNMP** em Monitor > **Listas de monitores**.
3. Associe um *tipo* de SNMP com um *conjunto* SNMP utilizando a lista suspensa **Implementação automática para** em Monitor > Conjuntos SNMP> Definir conjunto SNMP.
4. Execute um **LAN Watch** *(http://help.kaseya.com/webhelp/PTB/KDIS/R8/index.asp#1944.htm)*. Durante o LAN Watch, os dispositivos SNMP são atribuídos automaticamente para serem monitorados pelos conjuntos SNMP se o dispositivo SNMP retorna um valor para o objeto MIB `system.sysServices.0` que corresponda ao tipo SNMP associado com aqueles conjuntos SNMP.

Você também pode atribuir Conjuntos SNMP a dispositivos *manualmente*, do seguinte modo:

- Atribua um tipo SNMP para um dispositivo SNMP manualmente utilizando Monitor > Definir tipo SNMP. Isso faz com que os conjuntos SNMP que usarem o mesmo tipo comecem a monitorar o dispositivo SNMP.

# Como adicionar objetos SNMP

Ao selecionar objetos para inclusão em um conjunto SNMP, você tem a oportunidade de adicionar um novo objeto SNMP. Isso não deve ser necessário na maior parte dos casos, porque o **LAN Watch** *(http://help.kaseya.com/webhelp/PTB/KDIS/R8/index.asp#1944.htm)* recupera os objetos normalmente requeridos. Mas se precisa adicionar um objeto SNMP de um arquivo MIB manualmente, pode fazê-lo em Monitor > Adicionar objeto SNMP ou ao clicar no botão **Adicionar objeto...** durante a configuração de um conjunto SNMP.

A página **Árvore MIB SNMP** carrega um arquivo MIB (Management Information Base) e o exibe como uma *árvore* expansível de objetos MIB. Todos os objetos MIB são classificados por sua localização na árvore MIB. Uma vez carregado, você pode selecionar os objetos MIB que deseja instalar em seu VSA. Os fabricantes de dispositivos SNMP geralmente fornecem arquivos MIB em seus sites para os dispositivos que produzem.

> **Nota:** *Você pode rever a lista completa de objetos MIB já instalados ao selecionar a guia* **OIDs do MIB** *em Monitoramento > Listas de monitores. Essa é a lista de objetos MIB que você pode incluir atualmente em um conjunto SNMP.*

Se um fornecedor tiver fornecido um arquivo MIB, você pode seguir estas etapas:

1. Carregue o arquivo MIB do fornecedor clicando em **Carregar MIB...** Pode haver uma mensagem informando que há arquivos dependentes que precisam ser carregados primeiro. O fornecedor pode precisar fornecê-los também.
2. Clique nos ícones de expansão ⊞ na árvore MIB - *veja o gráfico de exemplo abaixo* - e encontrar os itens desejados a serem monitorados. Selecione cada caixa correspondente.
3. Clique em **Adicionar Objetos MIB** para mover os itens selecionados na Etapa 2 para a Lista de Objetos MIB.
4. Defina as configurações de monitoramento do novo objeto SNMP em um conjunto SNMP como faria normalmente.
5. O manuseio do número de objetos MIB na árvore pode tornar-se difícil rapidamente. Quando os objetos MIB desejados estiverem adicionados, o arquivo MIB poderá ser removido.

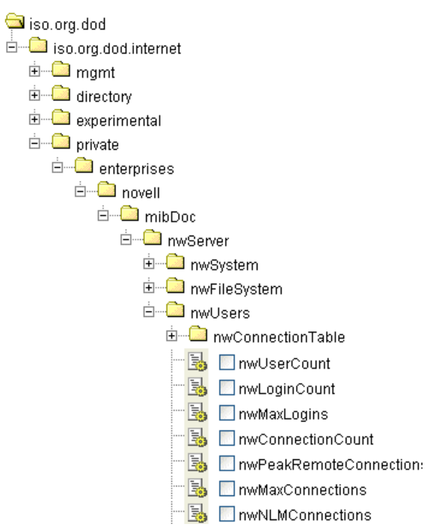
## Carregar MIB

Clique em **Carregar MIB...** para procurar e transferir um arquivo MIB. Quando um objeto MIB é adicionado, se o sistema ainda não tiver estes arquivos MIB II padrão, requeridos pela maioria dos MIBs, os carregará automaticamente: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Após os arquivos serem carregados, a árvore MIB localizada na base da página **Adicionar objeto SNMP** pode ser aberta e navegada para encontrar os novos objetos que o usuário pode selecionar. A maioria dos MIBs dos fornecedores privados é instalada na pasta `Private`. *Veja o exemplo gráfico abaixo*.

> **Nota:** O arquivo MIB pode ser carregado e removido a qualquer momento e *não* afeta nenhum objeto MIB utilizado nos conjuntos SNMP.

## Árvore MIB

A árvore MIB representa todos os objetos de arquivos MIB que estão atualmente carregados para o usuário selecionar.

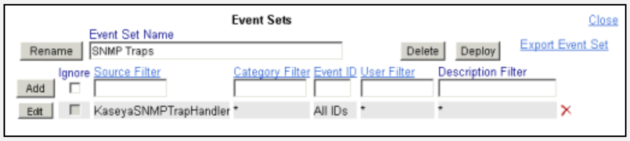



# Traps SNMP

A página **Alerta de interceptações SNMP** configura os alertas para uma máquina gerenciada, agindo como "escuta" de interceptações SNMP, quando detecta uma mensagem de **Interceptação SNMP**.

Quando **Alerta de interceptações SNMP** é atribuído a uma máquina gerenciada, o serviço denominado `Kaseya SNMP Trap Handler` é iniciado na máquina gerenciada. O serviço fica atento a mensagens de interceptação SNMP enviadas pelos dispositivos que permitem SNMP na mesma LAN. Cada vez que uma mensagem de interceptação SNMP é recebida pelo serviço, uma entrada de `Warning` de

interceptação SNMP é adicionada ao log de eventos do `Application` da máquina gerenciada. A **origem** destas entradas no log de eventos do `Application` é sempre `KaseyaSNMPTrapHandler`.

> **Nota:** *Crie um conjunto de eventos que inclua* `KaseyaSNMPTrapHandler` *como a* **origem**. *Use asteriscos* `*` *para os outros critérios se você não deseja filtrar ainda mais os eventos.*
>
> 
> 
>
> **Nota:** *SNMP utiliza a porta UDP padrão 162 para mensagens de interceptação SNMP. Assegure-se de que esta porta esteja aberta, caso utilize um firewall.*

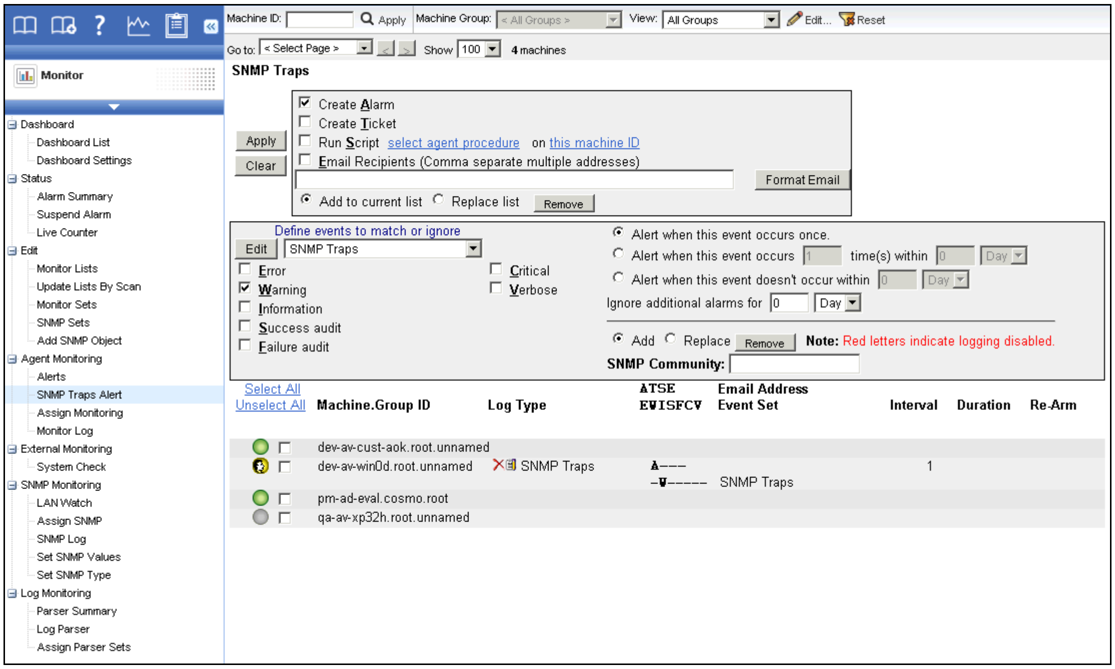
## Criar um alerta de interceptações SNMP

1. Selecione a página Monitor > **Alerta de interceptações de SNMP**.
2. Selecione o filtro **Conjunto de Eventos** usado para filtrar os evento que acionarão os alertas. Não selecione um conjunto de eventos para incluir *todos* os eventos de Interceptação SNMP.
3. Marque a caixa próxima da **categoria de evento** `Warning`. *Nenhuma outra categoria de evento é usada pelo alerta de interceptações SNMP.*

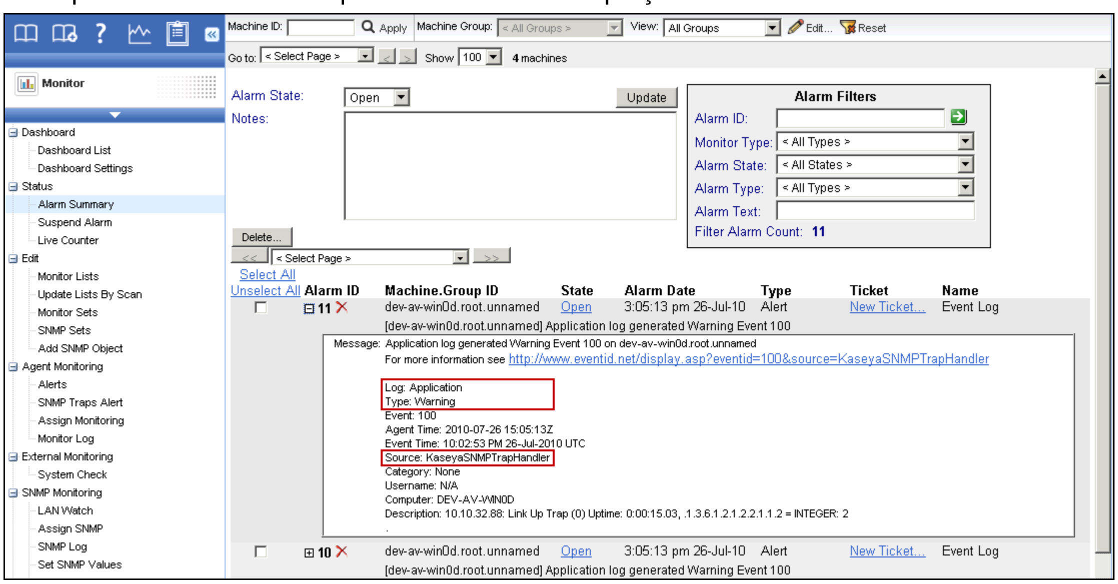
   > **Nota: Categorias de eventos** *realçadas em vermelho (EWISFCV) indicam que estas categorias de eventos não são coletadas pelo VSA.* **Alertas de log de eventos ainda são gerados mesmo que os logs de eventos não sejam coletados pelo VSA.**

4. Especifique a *frequência* da condição do alerta exigida para acionar um alerta:
   - **Alertar quando esse evento ocorrer uma vez.**
   - **Alertar quando este evento ocorrer <N> vezes dentro de <N> <períodos>**.
   - **Alertar quando este evento não ocorrer dentro de <N> <períodos>**.
   - **Ignorar alarmes adicionais para <N> <períodos>**.
5. Clique nas opções **Adicionar** ou **Substituir** e clique em **Aplicar** para atribuir alertas do tipo do evento selecionado às IDs de máquina selecionadas.
6. Clique em **Remover** para remover todos os alertas baseados em eventos das IDs de máquina selecionadas.

7. Ignorar o campo **Comunidade SNMP**. *Essa opção ainda não está implementada.*




Você pode analisar alarmes para alertas de interceptações SNMP em Monitor > Resumo de alarmes.



# Índice